Ce livre à été télécharger à www.phpmaroc.com

Rassembler à partir de:

www.cisco.com

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP afin de répondre aux exigences de conception		• Dépannage d'un équipement dans un réseau en fonctionnement	• Évaluation du processus de communication TCP/IP et de ses protocoles associés

Les logos et marques cités dans ce document sont la propriété de leurs auteurs respectifs

Copyright :

Ce tutorial est mis à disposition gratuitement au format HTML lisible en ligne par son auteur sur le site
http://www.cisco.com, son auteur préserve néanmoins tous ses droits de propriété intellectuelle.
Ce tutorial ne saurait être vendu, commercialisé, offert à titre gracieux, seul ou packagé, sous quelque forme que ce soit par une personne autre que son auteur sous peine de poursuite judiciaire.

L'auteur ne pourra pas être tenu responsable pour les dommages matériel ou immatériel, perte d'exploitation ou de clientèle liés à l'utilisation de ce tutorial.

1-Présentations des réseaux

Vue d'ensemble

Pour comprendre le rôle des ordinateurs dans un réseau, pensez à Internet. Les connexions à Internet sont essentielles dans les entreprises et les établissements d'enseignement. Il convient de planifier avec beaucoup de soin la construction d'un réseau permettant d'accéder à Internet. La connexion d'un ordinateur personnel (PC) à Internet requiert elle-même un minimum de réflexion et de planification préalables. Ainsi, les ressources informatiques nécessaires à cette connexion doivent être étudiées. Ceci inclut le type d'équipement – carte réseau ou modem – à utiliser pour connecter le PC à Internet. Il est également nécessaire de configurer les protocoles ou les règles permettant d'établir cette connexion. Enfin, la sélection d'un navigateur Internet approprié est importante.

Le présent module traite certains objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811. [2] [3] [4]

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP afin de répondre aux exigences de conception		• Dépannage d'un équipement dans un réseau en fonctionnement	• Évaluation du processus de communication TCP/IP et de ses protocoles associés

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP afin de répondre aux exigences de conception		• Dépannage d'un équipement dans un réseau en fonctionnement	

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Détermination des adresses IP • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur • Description et installation du matériel et du logiciel requis pour pouvoir communiquer via un réseau	• Mise en œuvre des connaissances mathématiques requises pour utiliser couramment les nombres entiers décimaux, binaires et hexadécimaux, ainsi que la logique binaire simple • Description du matériel et des logiciels requis pour pouvoir communiquer via un réseau • Utilisation des techniques d'adressage IP

Au terme de cette section, les étudiants doivent maîtriser les notions et les opérations suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
1.1	Connexion à Internet
1.2	Aspects mathématiques des réseaux

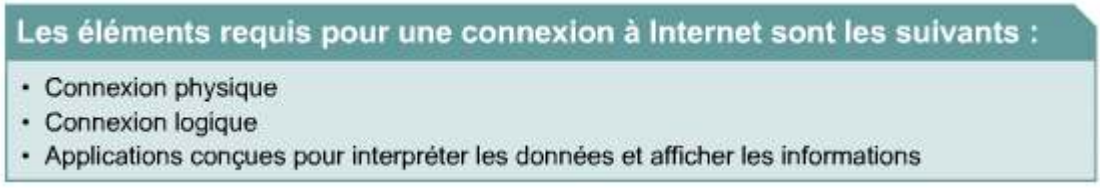
- Connaître la connexion physique à mettre en place pour relier un ordinateur à Internet
- Identifier les composants de l'ordinateur
- Installer les cartes réseau et/ou les modems et résoudre les problèmes pouvant les affecter
- Utiliser des procédures de test élémentaires pour vérifier le fonctionnement de la connexion à Internet
- Savoir utiliser les navigateurs Internet et les modules d'extension

1.1 Connexion à Internet

1.1.1 Éléments requis pour une connexion à Internet

Cette page présente les éléments physique et logique requis pour une connexion à Internet.

Internet représente le plus important réseau de données au monde. Il est formé d'une multitude de réseaux de plus ou moins grande taille reliée entre eux. Les ordinateurs personnels constituent les sources et les destinations de l'information qui circule sur Internet. La connexion à Internet englobe en réalité trois éléments: la connexion physique, la connexion logique et plusieurs applications. 1


Les éléments requis pour une connexion à Internet sont les suivants :
• Connexion physique
• Connexion logique
• Applications conçues pour interpréter les données et afficher les informations

Le premier élément implique de relier une carte d'interface de PC – modem ou carte réseau – à un réseau. La connexion physique assure le transfert des signaux entre les PC d'un réseau LAN et les équipements distants du réseau Internet.

La connexion logique, quant à elle, utilise des normes, plus précisément appelées protocoles. Un protocole correspond à un ensemble formel de règles et de conventions régissant le mode de communication des unités réseau entre elles. Les connexions à Internet font appel à plusieurs protocoles, parmi lesquels les protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*) sont les plus largement utilisés. Formant un ensemble, ces protocoles assurent conjointement la transmission des données ou des informations.

La connexion à Internet inclut enfin les applications, ou programmes logiciels, servant à interpréter les données et à les afficher sous une forme compréhensible. Ces applications utilisent les protocoles pour envoyer des données sur le réseau Internet et recevoir celles qui en émanent. Pour afficher le code HTML sous forme de page Web, un navigateur Internet, tel que Internet Explorer ou Netscape, est nécessaire. Le protocole FTP (*File Transfer Protocol*) permet, lui, de télécharger des fichiers et des programmes à partir d'Internet. Ajoutons enfin que les navigateurs Internet peuvent utiliser des modules d'extension pour afficher certains types de données comme les films ou les animations Flash.

Cette première présentation d'Internet peut laisser croire à une technologie et des processus exagérément simples. Au fur et à mesure qu'ils étudieront le sujet, les étudiants constateront cependant que la transmission de données via Internet est une opération complexe.

La page suivante présente les composants principaux d'un PC.

1.1 Connexion à Internet

1.1.2 Notions de base sur les PC

Les ordinateurs sont des éléments constitutifs importants d'un réseau. Pour cette raison, les étudiants doivent être en mesure d'en identifier les principaux composants. De nombreux équipements de réseau sont des ordinateurs à usage déterminé et contiennent un grand nombre de composants identiques à ceux d'un PC polyvalent.

Pour permettre d'accéder à des informations telles que des pages Web, un ordinateur doit fonctionner correctement. Les étudiants, qui seront amenés à résoudre des problèmes élémentaires concernant le matériel et les logiciels, doivent donc connaître certains composants, petits et discrets mais essentiels, d'un PC:

- **Transistor** – dispositif qui amplifie un signal ou qui ouvre et ferme un circuit.
- **Circuit intégré** – dispositif constitué d'un matériau semi-conducteur, qui contient de nombreux transistors et remplit une fonction précise.
- **Résistance –** composant électrique qui limite ou régule le flux de courant électrique dans un circuit électronique.
- **Condensateur** – composant électronique qui emmagasine de l'énergie sous forme de champ électrostatique ; il est constitué de deux plaques de métal conducteur séparées par un matériau isolant.
- **Connecteur** – partie d'un câble qui se branche sur un port ou une interface.
- **Diode électroluminescente ou LED *(Light Emitting Diode)*** – dispositif semi-conducteur qui émet de la lumière lorsqu'un courant le traverse.

Les étudiants doivent également se familiariser avec les sous-systèmes PC suivants:

- **Carte de circuits imprimés** – carte de circuits portant des pistes conductrices superposées, ou imprimées, sur l'une ou chacune de ses faces. Elle peut également comporter des couches internes pour le routage des signaux, ainsi que des plans de masse et d'alimentation. Des microprocesseurs, des puces, des circuits intégrés et d'autres composants électroniques sont montés sur la carte.
- **Lecteur de cédérom** – unité permettant de lire les informations stockées sur un cédérom.
- **Processeur** – unité de contrôle et de calcul d'un ordinateur. Le processeur assure l'interprétation et l'exécution des instructions en plus d'effectuer les opérations logiques et mathématiques. 1



- **Lecteur de disquette** – unité de l'ordinateur, assurant la lecture et l'écriture de données sur un disque de plastique souple de 3,5 pouces, recouvert de métal. La capacité de stockage d'une disquette standard est d'environ 1 Mo de données. 2



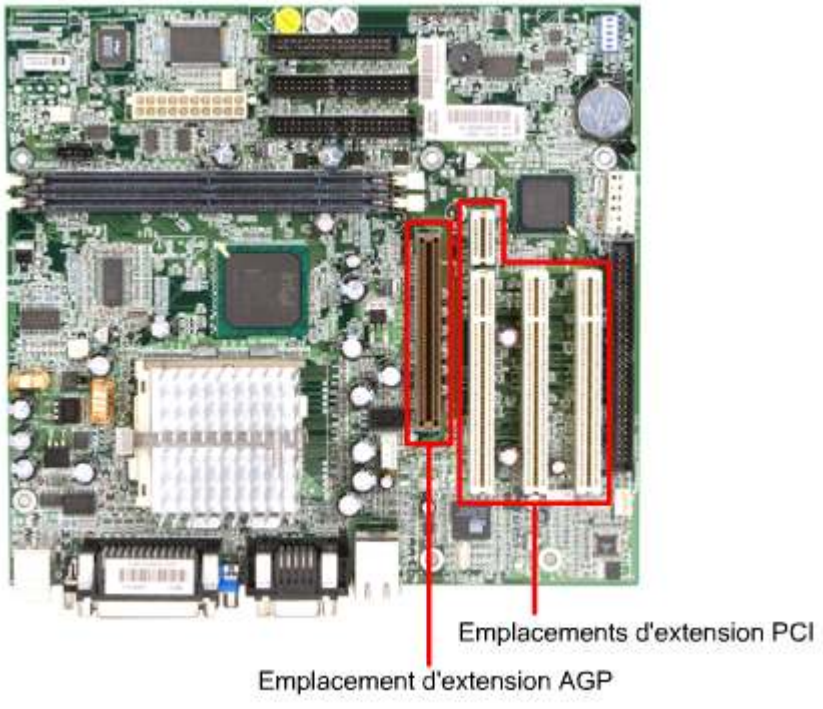
- **Unité de disque dur** – dispositif de stockage de l'ordinateur, utilisant un empilement de plateaux recouverts d'une surface magnétisée pour enregistrer des données ou des programmes. Il existe des disques durs de différentes capacités.
- **Microprocesseur** – processeur de très petite taille, dont les éléments sont fixés sur une puce de silicium spéciale. Le microprocesseur utilise la technologie de l'intégration à très grande échelle (*VLSI – Very Large-Scale Integration*) pour réunir la mémoire, l'unité logique et l'unité de contrôle de l'ordinateur sur une seule puce.
- **Carte mère** – principale carte de circuits imprimés d'un ordinateur. Elle contient le bus, le microprocesseur et les circuits intégrés utilisés pour contrôler les périphériques tels que le clavier, les dispositifs d'affichage graphique et de texte, les ports série et parallèles, une manette de jeu et la souris. 3



- **Bus** – ensemble de lignes électriques sur la carte mère, permettant le transfert de données et de signaux de synchronisation entre les différents éléments d'un ordinateur.
- **Mémoire vive (RAM)** – également désignée sous le nom de mémoire en lecture/écriture, elle permet l'enregistrement de nouvelles données et la lecture des données

stockées. Cette mémoire nécessite une alimentation électrique pour assurer la conservation des données. En cas de mise hors tension de l'ordinateur ou de coupure de courant, toutes les données stockées dans la mémoire RAM sont perdues.

- **Mémoire morte (ROM)** – mémoire de l'ordinateur qui contient des données pré-enregistrées. Les données stockées sur la puce de mémoire ROM sont accessibles uniquement en lecture et ne peuvent pas être supprimées.
- **Unité centrale** – partie principale d'un PC, comprenant le châssis, le microprocesseur, la mémoire centrale, le bus et les ports. Le clavier, le moniteur et les différents périphériques externes connectés à l'ordinateur ne font pas partie de l'unité centrale.
- **Emplacement d'extension** – fente d'extension permettant d'insérer une carte de circuits sur la carte mère pour augmenter les capacités de l'ordinateur. La figure 4 présente des emplacements d'extension PCI (*Peripheral Component Interconnect*) et AGP (*Accelerated Graphics Port*). La spécification PCI assure une connexion rapide utilisée notamment pour les cartes réseau, les modems internes et les cartes vidéo. Le port AGP quant à lui offre une connexion à haut débit entre le dispositif graphique et la mémoire système. Il permet une connexion rapide utilisée pour l'infographie tridimensionnelle.



- **Alimentation** – composant qui fournit le courant à l'ordinateur.

Les composants de fond de panier ci-après sont également importants:

- **Fond de panier** – carte de circuits électroniques offrant des circuits et des connecteurs pour le branchement de cartes d'équipements électroniques supplémentaires ; dans un ordinateur, le fond de panier est généralement synonyme de la carte mère ou compris dans celle-ci.
- **Carte réseau** – carte d'extension installée dans un ordinateur pour pouvoir connecter ce dernier à un réseau.
- **Carte vidéo** – carte installée dans un PC et qui lui donne ses capacités d'affichage.
- **Carte son** – carte d'extension permettant à un ordinateur de gérer et de produire des sons.
- **Port parallèle** – port capable de transférer plusieurs bits à la fois. Il est utilisé pour connecter des unités externes telles que des imprimantes.
- **Port série** – ce port, qui ne transmet qu'un seul bit à la fois, peut être utilisé pour la communication série.
- **Port souris** – port utilisé pour connecter une souris à un ordinateur.
- **PortUSB** – connecteur pour périphérique USB (*Universal Serial Bus*). Ce port permet de connecter aisément et rapidement un périphérique comme une souris ou une imprimante à l'ordinateur.

- **Firewire** – norme d'interface série qui garantit des communications à haut débit et offre des services de données en temps réel, transmises en mode isochrone.
- **Cordon d'alimentation** – cordon servant à brancher un équipement électrique sur une prise de courant qui alimente l'équipement en électricité.

Considérez les composants internes d'un PC comme un réseau d'équipements, tous reliés au bus système.

Grâce aux travaux pratiques, les étudiants apprendront à trouver et identifier les différents composants d'un PC.

La page suivante propose des informations sur les cartes réseau.

Activité de TP

Exercice: Matériel de l'ordinateur

Ce TP traite des principaux périphériques d'un PC et des connexions de celui-ci, notamment la connexion au réseau

1.1 Connexion à Internet

1.1.3 Carte réseau

Cette page définit une carte réseau et décrit son fonctionnement. Elle permet également d'apprendre à choisir la carte réseau la plus appropriée à un PC.

Une carte réseau, également nommée adaptateur réseau, est nécessaire à l'ordinateur pour envoyer des informations au réseau et en recevoir de celui-ci. Dans les ordinateurs de bureau, il s'agit d'une carte de circuits imprimés insérée dans un emplacement de la carte mère pour établir la connexion avec le média réseau 1



Dans les ordinateurs portables, ce composant est généralement intégré à l'ordinateur ou disponible sous la forme d'une carte PCMCIA aussi petite qu'une carte de crédit 2



Les cartes PCMCIA (*Personal Computer Memory Card International Association*) sont également désignées sous le nom de cartes PC. Le type de carte doit être choisi en fonction du média et du protocole utilisés par le réseau local.

La carte communique avec le réseau via une connexion série et avec l'ordinateur par le bus interne de celui-ci. Elle utilise une demande d'interruption ou IRQ, une adresse d'entrée/sortie (E/S) et de l'espace en mémoire

haute pour communiquer avec le système d'exploitation. Une valeur d'IRQ (*Interrupt Request*) désigne une adresse donnée, utilisée par un périphérique particulier pour interrompre le processeur et lui envoyer des signaux sur son fonctionnement. Ainsi, lorsqu'une imprimante termine un travail d'impression, elle envoie un signal d'interruption à l'ordinateur. Durant cette interruption momentanée, l'ordinateur peut décider du processus suivant à exécuter. Pour éviter toute confusion liée à l'envoi de plusieurs signaux à l'ordinateur via une même ligne d'interruption, il est nécessaire de spécifier, pour chaque périphérique, une valeur d'IRQ unique et la ligne reliant ce composant à l'ordinateur. Avant l'apparition des périphériques «plug-and-play», les utilisateurs devaient souvent définir manuellement les valeurs d'IRQ ou connaître ces valeurs pour pouvoir installer un nouveau périphérique sur un ordinateur.

Les critères ci-après sont à prendre en compte pour choisir une carte réseau :

- **Protocoles** – Ethernet, Token Ring ou FDDI.
- **Types de média** – câble à paires torsadées, câble coaxial ou fibre optique.
- **Type de bus système** – PCI ou ISA.

Utilisez l'activité de média interactive pour afficher une carte réseau.

La page qui suit décrit l'installation d'une carte réseau et d'un modem.

Activité de média interactive

Agrandissement: Carte réseau

Cet agrandissement vous permet d'observer les détails d'une carte réseau.

1.1 Connexion à Internet

1.1.4 Installation d'une carte réseau et d'un modem

Cette page explique de quelle façon un adaptateur, qui peut être un modem ou une carte réseau, assure la connectivité à Internet. Elle apprend également aux étudiants à installer ce type de composant.

Le modem, ou modulateur-démodulateur, est un équipement nécessaire pour relier l'ordinateur à une ligne téléphonique. Il convertit les signaux numériques formés par les données issues de l'ordinateur en signaux analogiques compatibles avec une ligne téléphonique standard. Dans l'ordinateur qui reçoit les données, le modem démodule les signaux, autrement dit les retransforme en données numériques. Les modems peuvent être installés comme des composants internes 1



ou reliés de manière externe à l'ordinateur et connectés à une ligne téléphonique. 2

Tout équipement inclus dans un réseau doit être pourvu d'une carte réseau, qui réalise l'interface entre chaque hôte et le réseau. Plusieurs types de cartes sont disponibles selon les configurations des équipements du réseau. La figure 3

présente des cartes PCMCIA avec et sans fil, ainsi qu'un adaptateur Ethernet USB (*Universal Serial Bus*). Les ordinateurs de bureau utilisent un adaptateur interne 4, appelé carte réseau, ou un adaptateur externe 5

qui assure la connexion au réseau via un port USB.



Les situations suivantes requièrent l'installation d'une carte réseau :

- Installation sur un PC qui n'en est pas encore pourvu.
- Remplacement d'une carte endommagée ou qui présente un dysfonctionnement.
- Mise à niveau d'une carte réseau de 10 Mbits/s vers une carte de 10/100/1000 Mbits/s.
- Installation d'une carte de type différent, par exemple sans fil.
- Ajout d'une carte secondaire ou de secours pour garantir la sécurité du réseau.

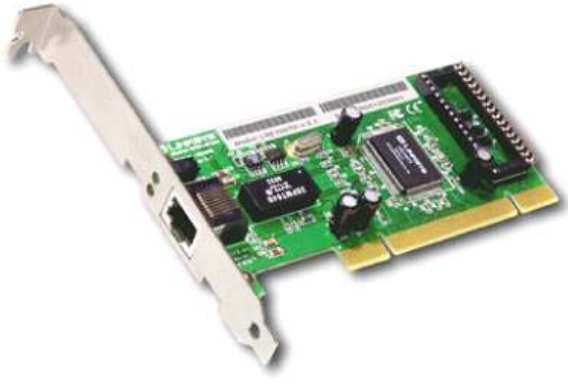
Les conditions ci-après peuvent être nécessaires à l'installation d'une carte réseau ou d'un modem :

- Connaissance de la configuration de l'adaptateur, des cavaliers et des logiciels plug-and-play.
- Disponibilité d'outils de diagnostic.
- Capacité à résoudre des conflits entre ressources matérielles.



La page suivante présente l'historique de la connectivité des réseaux.





1.1 Connexion à Internet

1.1.5 Vue d'ensemble des solutions de connectivité haut débit et commutée

Cette page décrit l'évolution des technologies de connectivité, des modems aux services à haut débit. 1

Vue d'ensemble des solutions de connectivité

- Les modems ont été lancés au début des années 1960 pour connecter des terminaux passifs à un ordinateur central
- Dans les années 1970, les systèmes BBS (Bulletin Board System) offraient des services informatisés d'échange d'informations, auxquels les utilisateurs pouvaient se connecter pour envoyer et consulter des messages
- Les années 1980 ont vu naître le besoin de transférer des fichiers et des graphiques
- Au cours des années 1990, la vitesse des modems est passée à 56 Kbits/s
- En 2000, la demande de services à haut débit s'est développée

Apparus au début des années 1960, les modems servaient à connecter des terminaux passifs à un ordinateur central. De nombreuses entreprises recouraient alors à la location de services de traitement informatique car le coût à payer pour posséder un système sur site était trop élevé. La connexion par modem atteignait une vitesse de 300 bits par seconde (bits/s) seulement, ce qui correspond à environ 30 caractères par seconde.

Dans les années 1970, le prix des PC est devenu plus abordable et les systèmes BBS (*Bulletin Board System*) sont apparus. Ces systèmes offraient des services informatisés d'échange d'informations, auxquels les utilisateurs pouvaient se connecter notamment pour afficher des messages et y répondre. La vitesse de 300 bits/s était acceptable puisqu'elle était supérieure à la capacité de lecture à l'écran ou de frappe au clavier des utilisateurs. Au début des années 1980, l'utilisation des BBS a connu un développement exponentiel et la vitesse de 300 bits/s s'est rapidement avérée insuffisante pour le transfert de fichiers et de graphiques volumineux. Dans les années 1990, le débit des modems est passée à 9 600 bits/s. En 1998, la vitesse standard actuelle de 56 000 bits/s, ou 56 Kbits/s, a été atteinte. Les services à haut débit utilisés dans les environnements d'entreprise, tels que la technologie DSL (*Digital Subscriber Line*) et les connexions par modem câble, sont ensuite devenus accessibles aux particuliers. Ces services ne requièrent plus d'équipement coûteux ni de ligne téléphonique supplémentaire. Toujours actifs, ils offrent un accès instantané à Internet et ne requièrent pas d'établir une nouvelle connexion à chaque session. Ces avancées technologiques, garantes d'une fiabilité et d'une flexibilité accrues, ont simplifié la mise en place de connexions partagées à Internet dans les réseaux domestiques ou de petites entreprises.

La page suivante décrit l'un des principaux ensembles de protocoles réseau.

1.1 Connexion à Internet

1.1.6 TCP/IP: Description et configuration

Cette page présente le standard TCP/IP (*Transmission Control Protocol/Internet Protocol*). 1

- TCP/IP désigne une suite de protocoles élaborés pour assurer le partage des ressources entre les ordinateurs
- Les outils du système d'exploitation permettent de définir les paramètres TCP/IP

TCP/IP désigne un ensemble de protocoles et de règles mis au point pour permettre aux ordinateurs de partager les ressources d'un réseau. Pour configurer cet ensemble de protocoles sur une station de travail, il convient

d'utiliser les outils du système d'exploitation. Le processus de configuration diffère très peu d'un système d'exploitation Windows à un système d'exploitation Macintosh.

L'activité de TP porte sur l'affichage des informations de configuration TCP/IP essentielles.

La page suivante décrit la commande **ping**.

Activité de TP

Exercice: Configuration des paramètres TCP/IP d'un réseau

Ce TP vous permet d'identifier les différents outils à utiliser – selon le système d'exploitation – pour connaître la configuration d'un réseau

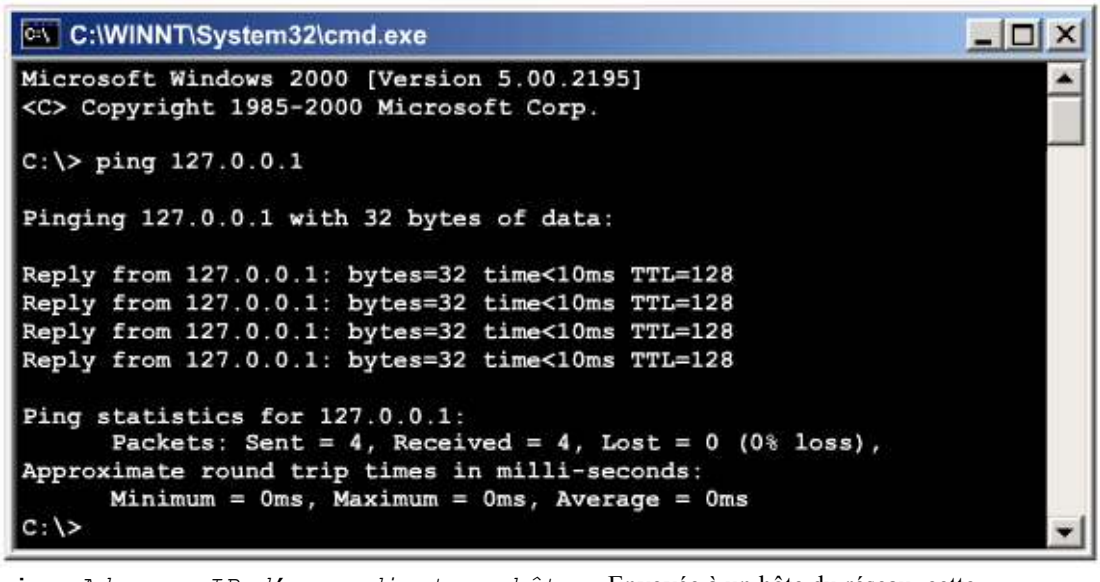
1.1 Connexion à Internet
1.1.7 Test de connectivité avec la commande ping

Cette page explique comment utiliser la commande **ping** pour tester la connectivité du réseau.

La commande ping lance un utilitaire qui vérifie l'existence d'une adresse IP et son accessibilité. Cet utilitaire fonctionne sur le modèle du sonar et tire également son nom de l'analogie avec le bruit émis par cet appareil.

La commande **ping** utilise des paquets de données IP (*Internet Protocol*) spéciaux, nommés datagrammes ICMP (*Internet Control Message Protocol*), pour envoyer des messages de demande d'écho à une destination donnée. Chaque paquet envoyé équivaut à une demande de réponse. La réponse renvoyée indique le taux de réussite et le temps de parcours aller-retour entre les équipements source et de destination. 1 Ces informations déterminent la connectivité avec l'équipement de destination. La commande **ping** sert à tester les fonctions de transmission et de réception de la carte réseau, la configuration TCP/IP et la connectivité réseau. Les différentes utilisations possibles de la commande ping sont les suivantes :

- **ping** *127.0.0.1* – Utilisée pour tester la boucle locale interne, cette commande permet de vérifier la configuration réseau TCP/IP. 1



- **ping** *Adresse IP d'un ordinateur hôte* – Envoyée à un hôte du réseau, cette commande vérifie la configuration de l'adresse TCP/IP pour l'hôte et la connectivité avec ce dernier.

- **ping** *Adresse IP de la passerelle par défaut* – L'exécution de la commande ping vers la passerelle par défaut sert à vérifier si le routeur qui relie le réseau local à d'autres réseaux est accessible.
- **ping** *Adresse IP d'un hôte distant* – Permet de tester la connectivité avec un hôte distant.

L'activité de TP porte sur l'utilisation des commandes **ping** et **tracert**.

La page suivante traite des navigateurs Web.



Activité de TP

Exercice: Utilisation des commandes **ping** et **tracert** à partir d'une station de travail

Ce TP vous apprend à exécuter les commandes **ping** et **tracert** (Traceroute) sur une station de travail

1.1 Connexion à Internet

1.1.8 Navigateurs Web et modules d'extension

Cette page décrit un navigateur Web et la façon dont il exécute les fonctions suivantes:

- Contacter un serveur Web
- Demander des informations
- Recevoir des informations
- Afficher les résultats à l'écran

Un navigateur Web est un logiciel conçu pour interpréter le langage HTML – l'un des langages utilisés pour coder le contenu des pages Web. Certaines technologies nouvelles font appel à d'autres langages de balisage offrant des fonctionnalités plus perfectionnées. Le langage le plus couramment utilisé demeure toutefois le HTML, qui permet d'afficher des graphiques, de lire des fichiers audio ainsi que des films et d'exécuter d'autres fichiers multimédia. Les liens hypertexte incorporés dans une page Web permettent d'accéder rapidement à un emplacement différent dans une même page ou à une adresse Internet différente.

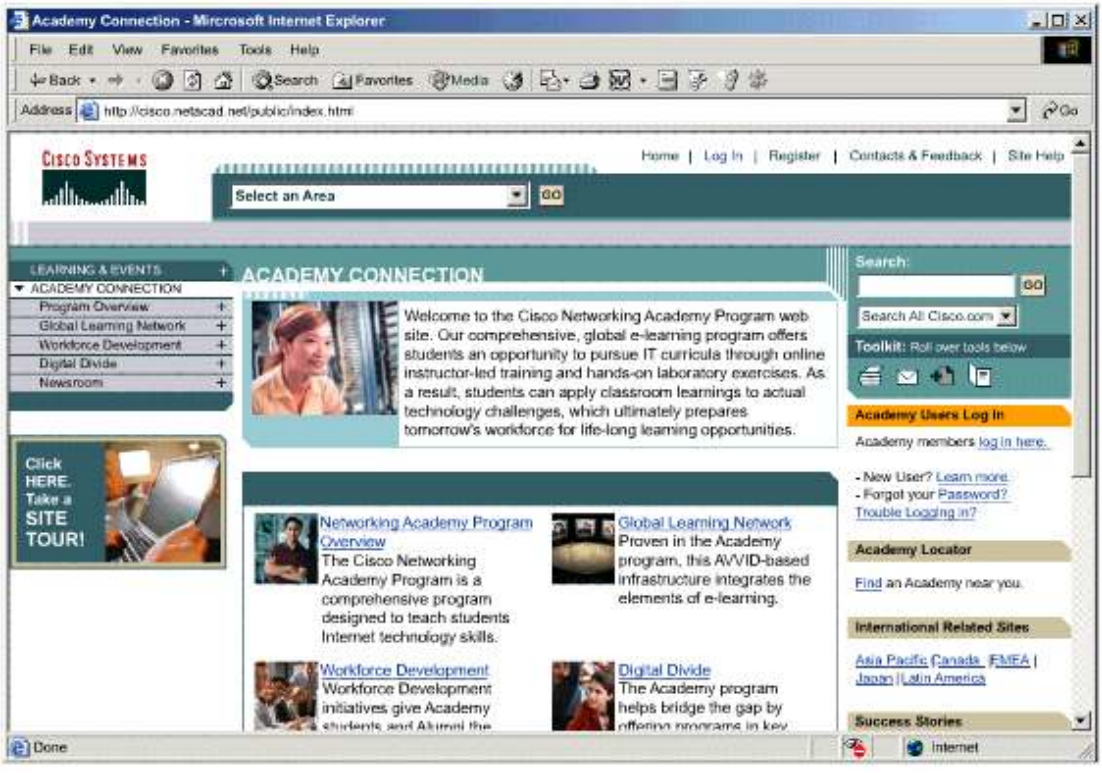
Microsoft Internet Explorer et Netscape Communicator sont deux des navigateurs Web les plus utilisés. Ces deux produits effectuent les mêmes opérations mais diffèrent toutefois sur quelques points. Certains sites Web, développés spécifiquement pour l'un des navigateurs, ne permettent pas l'affichage dans un autre produit. Il est donc préférable d'installer les deux programmes sur son ordinateur.

Les caractéristiques principales de Netscape Navigator sont les suivantes: 1


Academy Connection - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
http://cisco.netacad.net/public/index.html
Search
Cisco Systems
Home | Log In | Register | Contacts & Feedback | Site Help
Select an Area
GO
LEARNING & EVENTS
ACADEMY CONNECTION
Program Overview
Global Learning Network
Workforce Development
Digital Divide
Newsroom
ACADEMY CONNECTION
Welcome to the Cisco Networking Academy Program web site. Our comprehensive, global e-learning program offers students an opportunity to pursue IT curricula through online instructor-led training and hands-on laboratory exercises. As a result, students can apply classroom learnings to actual technology challenges, which ultimately prepares tomorrow's workforce for life-long learning opportunities.
Click HERE. Take a SITE TOUR!
Networking Academy Program Overview
The Cisco Networking Academy Program is a comprehensive program designed to teach students Internet technology skills.
Global Learning Network
Proven in the Academy program, this AVVID-based infrastructure integrates the elements of e-learning.
Workforce Development
Workforce Development initiatives give Academy students and Alumni the
Digital Divide
The Academy program helps bridge the gap by offering programs in key
Search:
GO
Search All Cisco.com
Toolkit: Roll over tools below
Academy Users Log In
Academy members log in here.
- New User? Learn more.
- Forgot your Password?
Trouble Logging In?
Academy Locator
Find an Academy near you.
International Related Sites
Asia Pacific | Canada | EMEA | Japan | Latin America
Success Stories
Document: Done (1.265 secs)

- Fut le premier navigateur très répandu.
- Occupe moins d'espace disque.
- Affiche les fichiers HTML.
- Prend en charge le transfert de fichiers, le courrier électronique et d'autres fonctions.

Caractéristiques d'Internet Explorer (IE):


Academy Connection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://cisco.netscad.net/public/index.html
Cisco Systems
Home | Log In | Register | Contacts & Feedback | Site Help
Select an Area
GO
LEARNING & EVENTS
ACADEMY CONNECTION
Program Overview
Global Learning Network
Workforce Development
Digital Divide
Newsroom
ACADEMY CONNECTION
Welcome to the Cisco Networking Academy Program web site. Our comprehensive, global e-learning program offers students an opportunity to pursue IT curricula through online instructor-led training and hands-on laboratory exercises. As a result, students can apply classroom learnings to actual technology challenges, which ultimately prepares tomorrow's workforce for life-long learning opportunities.
Click HERE. Take a SITE TOUR!
Networking Academy Program Overview
The Cisco Networking Academy Program is a comprehensive program designed to teach students Internet technology skills.
Global Learning Network
Proven in the Academy program, this AVVID-based infrastructure integrates the elements of e-learning.
Workforce Development
Workforce Development initiatives give Academy
Digital Divide
The Academy program helps bridge the gap by
Search:
GO
Search All Cisco.com
Toolkit: Roll over tools below
Academy Users Log In
Academy members log in here.
- New User? Learn more.
- Forgot your Password?
Trouble Logging in?
Academy Locator
Find an Academy near you.
International Related Sites
Asia Pacific | Canada | EMEA | Japan | Latin America
Success Stories
Done
Internet

- Étroitement intégré aux autres produits Microsoft.
- Occupe davantage d'espace disque.
- Affiche les fichiers HTML.
- Prend en charge le transfert de fichiers, le courrier électronique et d'autres fonctions.

Il existe également de nombreux types de fichier spéciaux ou propriétaires que les navigateurs Web standard ne peuvent pas afficher. Dans ce cas, il est nécessaire de configurer les navigateurs pour activer l'utilisation de modules d'extension. Ces derniers fonctionnent conjointement avec les navigateurs et lancent les programmes requis par les fichiers spéciaux.

- **Flash** – exécute les fichiers multimédia créés avec Macromedia Flash.
- **Quicktime** – exécute les fichiers vidéo créés avec Apple.
- **Real Player** – lit les fichiers audio.

Pour installer le module d'extension Flash, procédez comme suit:

1. Accédez au site Web de Macromedia.
2. Téléchargez la dernière version du fichier d'installation du module d'extension.
3. Lancez l'installation du module d'extension dans Netscape ou Internet Explorer.
4. Accédez au site Web Cisco Networking Academy Program pour vérifier que l'installation s'est déroulée correctement et que le module fonctionne.

Parmi leurs utilités multiples, les ordinateurs offrent également à de nombreux employés la possibilité d'exploiter plusieurs applications proposées sous la forme d'une suite bureautique telle que Microsoft Office. Ces applications sont généralement les suivantes :

- Le tableur contient des tableaux constitués de colonnes et de lignes. Ce type de programme est souvent utilisé avec des formules pour traiter et analyser les données.
- Le traitement de texte est une application servant à créer et à modifier des documents texte. Les traitements de texte modernes permettent de créer des documents comportant des images et des mises en forme complexes.
- Le logiciel de gestion de base de données permet de stocker, de mettre à jour, d'organiser, de trier et de filtrer des enregistrements. Un enregistrement est un ensemble d'informations identifiées par un sujet commun tel que le nom d'un client.
- Le logiciel de présentation est utilisé pour concevoir et élaborer des exposés qui seront présentés lors de réunions, devant une classe ou devant des clients.
- Le gestionnaire personnel offre généralement des fonctions de courrier et de carnet d'adresses, un agenda, ainsi qu'une liste de tâches.

A l'instar des machines à écrire avant l'apparition des PC, les applications bureautiques font aujourd'hui partie de notre environnement de travail quotidien.

L'activité de TP vous aide à comprendre le fonctionnement d'un navigateur Web.

La page suivante aborde la procédure de dépannage.

Activité de TP

Exercice: Notions de base sur les navigateurs Web

Ce TP vous apprend à utiliser un navigateur Web pour accéder à des sites Internet et vous familiarise avec la notion d'URL.

1.1 Connexion à Internet

1.1.9 Résolution des problèmes de connexion à Internet

1. Définition du problème
2. Recueil des données factuelles
3. Étude des possibilités
4. Conception d'un plan d'action
5. Mise en œuvre du plan
6. Observation des résultats
7. Enregistrement des résultats dans des documents
8. Introduction de problèmes et dépannage

L'activité de TP proposée sur cette page porte sur la résolution de problèmes liés au matériel, aux logiciels et à la configuration du réseau. Il s'agit de localiser les problèmes et de prendre les mesures requises dans le délai imparti, afin d'accéder au contenu du cursus. Ce TP illustre la complexité des opérations à accomplir pour configurer un accès à Internet. Parmi ces opérations figurent notamment les processus et les procédures à exécuter pour le dépannage du matériel, des logiciels et des systèmes réseau.

Cette leçon est terminée. La leçon suivante aborde les systèmes de numération utilisés par les ordinateurs. La première page est consacrée au système binaire.

Activité de TP

Exercice: Procédure élémentaire de dépannage PC/réseau

Ce TP enseigne la démarche à respecter pour dépanner les ordinateurs et les réseaux et vous familiarise avec les problèmes matériels et logiciels les plus courants

1.2 Aspects mathématiques des réseaux

1.2.1 Présentation binaire des données

Cette page décrit l'utilisation du système de numération binaire par les ordinateurs pour représenter les données.

Les ordinateurs gèrent et stockent les données à l'aide de commutateurs électroniques pouvant prendre deux états : « En fonction » et « Hors fonction » (ON et OFF). Ils ne peuvent traiter que les données répondant à ce format à deux états, dit binaire. Les chiffres 0 et 1 servent à représenter les deux états possibles d'un composant électronique de l'ordinateur. La valeur 1 correspond à l'état En fonction et la valeur 0, à l'état Hors fonction. Ces valeurs sont appelées chiffres binaires ou bits.

Le code ASCII (*American Standard Code for Information Interchange*) – code le plus couramment utilisé pour représenter les données alphanumériques dans les ordinateurs – 1

Clavier	Code binaire
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000

emploie des chiffres binaires pour symboliser les caractères saisis au clavier. Les 0 et les 1 désignant les états Hors fonction et En fonction sont transmis par les ordinateurs d'un réseau sous la forme d'ondes électriques, lumineuses ou radio. Il est important de savoir que chaque caractère du clavier est représenté par une combinaison unique de huit chiffres binaires qui lui est propre. 2

Caractère	Valeur ASCII	Binaire
a	97	01100001

Les ordinateurs étant conçus pour fonctionner avec des commutateurs En fonction/Hors fonction, ils sont naturellement capables de traiter des chiffres et des nombres binaires. Les humains quant à eux utilisent le système décimal, système relativement simple comparé aux longues séries de 1 et de 0 traitées par les ordinateurs. Par conséquent, les ordinateurs doivent pouvoir effectuer la conversion entre les nombres binaires et les nombres décimaux.

Les nombres binaires sont parfois convertis en nombres hexadécimaux (hex), ce qui permet de réduire une longue chaîne de chiffres binaires en quelques caractères hexadécimaux. Ces derniers sont plus simples à mémoriser et à manipuler.

La page suivante aborde les bits et les octets.

1.2 Aspects mathématiques des réseaux

1.2.2 Bits et octets

Cette page définit les bits et les octets.

Le chiffre binaire 0 est représenté par une tension électrique de 0 volts.

Le chiffre binaire 1 est représenté par une tension électrique de +5 volts.

Les ordinateurs sont conçus pour traiter des groupes de huit bits, chaque groupe constituant un octet [1].

Unités	Définition	Octets*	Bits*	Exemples
Bit (b)	Chiffre binaire, égal à 1 ou 0	1	1	En fonction/Hors fonction ; Ouvert/Fermé ; +5 volts ou 0 volt
Octet (o)	8 bits	1	8	La lettre X en code ASCII
Kilo-octet (Ko)	1 kilo-octet = 1 024 octets	1000	8,000	Email type = 2 Ko Rapport de 10 pages = 10 Ko
Méga-octet (Mo)	1 méga-octet = 1 024 kilo-octets = 1 048 576 octets	1 million	8 millions	Disquettes = 1,44 Mo RAM standard = 32 Mo Cédérom = 650 Mo
Gigaoctet (Go)	1 gigaoctet = 1 024 méga-octets = 1 073 741 824 octets	1 milliard	8 milliards	Disque dur type = 40 Go ou plus
Téraoctet (To)	1 téraoctet = 1 024 gigaoctets = 1 099 511 627 778 octets	1 billion	8 billions	Quantité théorique de données transmissibles par fibre optique en une seconde

* Nombre d'octets ou de bits habituel ou approximatif

Dans un ordinateur, un octet représente un emplacement de mémoire adressable unique. Chacun de ces emplacements correspond à une valeur ou un caractère unique de données, tel qu'un caractère du code ASCII. Les huit commutateurs susceptibles de prendre chacun la valeur 0 ou 1 peuvent donner lieu à un nombre total de 256 combinaisons.

La page suivante décrit le système de numération décimal.

1.2 Aspects mathématiques des réseaux

1.2.3 Système de numération décimal

Un système de numération consiste en un ensemble de symboles dont l'utilisation est définie par des règles. Cette page traite du système de numération le plus largement utilisé – le système décimal ou système à base 10.

La base 10 utilise les dix symboles 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9, qu'elle permet de combiner pour représenter toutes les valeurs numériques possibles.

Le système de numération décimal repose sur les puissances de 10. Dans un nombre, que l'on doit lire de droite à gauche, chaque chiffre est multiplié par le nombre de base 10, élevé à une certaine puissance (l'exposant). La puissance à laquelle on élève la base 10 dépend du rang occupé par le chiffre à gauche de la virgule décimale. La lecture d'un nombre décimal en partant de la droite fournit les informations suivantes : le tout premier rang à droite (rang numéro 0) correspond à 10^0, qui est égal à 1 ; le deuxième rang (rang n° 1) correspond à 10^1 qui est égal à 10 ; le troisième rang (rang n° 2) correspond à 10^2, qui est égal à 100 ; ainsi de suite jusqu'au septième rang (rang n° 6), qui correspond à 10^6, c'est-à-dire à 1 000 000. Ces règles s'appliquent quel que soit la longueur d'un nombre. 1

Valeur des rangs	1000 100 10 1
Base Exposant	$10^3 = 1000$ $10^2 = 100$ $10^1 = 10$ $10^0 = 1$
Nombre de symboles	10
Symboles	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Fondement	Les êtres humains ont généralement 10 doigts

Voici un exemple:

$2134 = (2 \times 10^3) + (1 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$

Cette révision du système décimal vise à faciliter la compréhension des systèmes à base 2 et à base 16, qui fonctionnent selon les mêmes règles.

La page suivante décrit le système de numération à base 2.

1.2 Aspects mathématiques des réseaux

1.2.4 Système de numération à base 2

Cette page définit le système de numération utilisé par les ordinateurs pour reconnaître et traiter les données : le système binaire ou système à base 2. 1

Valeur des rangs	128 64 32 16 8 4 2 1
Base Exposant	$2^7 = 128$ $2^3 = 8$ $2^6 = 64$ $2^2 = 4$ $2^5 = 32$ $2^1 = 2$ $2^4 = 16$ $2^0 = 1$
Nombre de symboles	2
Symboles	0, 1
Fondement	Les systèmes à transistors à deux états de tension (binaire discret) sont multiples, efficaces, peu coûteux, à faible encombrement et présentent une certaine immunité aux interférences (bruit).

Le système binaire utilise seulement deux symboles, le 0 et le 1. Dans un nombre binaire lu de droite à gauche, le rang de chaque chiffre correspond à 2, le nombre de base, élevé à la puissance (exposant) 0, puis à la puissance 1 et ainsi de suite jusqu'à la puissance 7. Les valeurs respectives des rangs, de droite à gauche, sont donc les suivantes : 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6 et 2^7, ou 1, 2, 4, 8, 16, 32, 64 et 128.

Voici un exemple:

$10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22\ (16 + 0 + 4 + 2 + 0)$

Cet exemple montre que le nombre 10110 en base 2 est égal au nombre décimal 22.

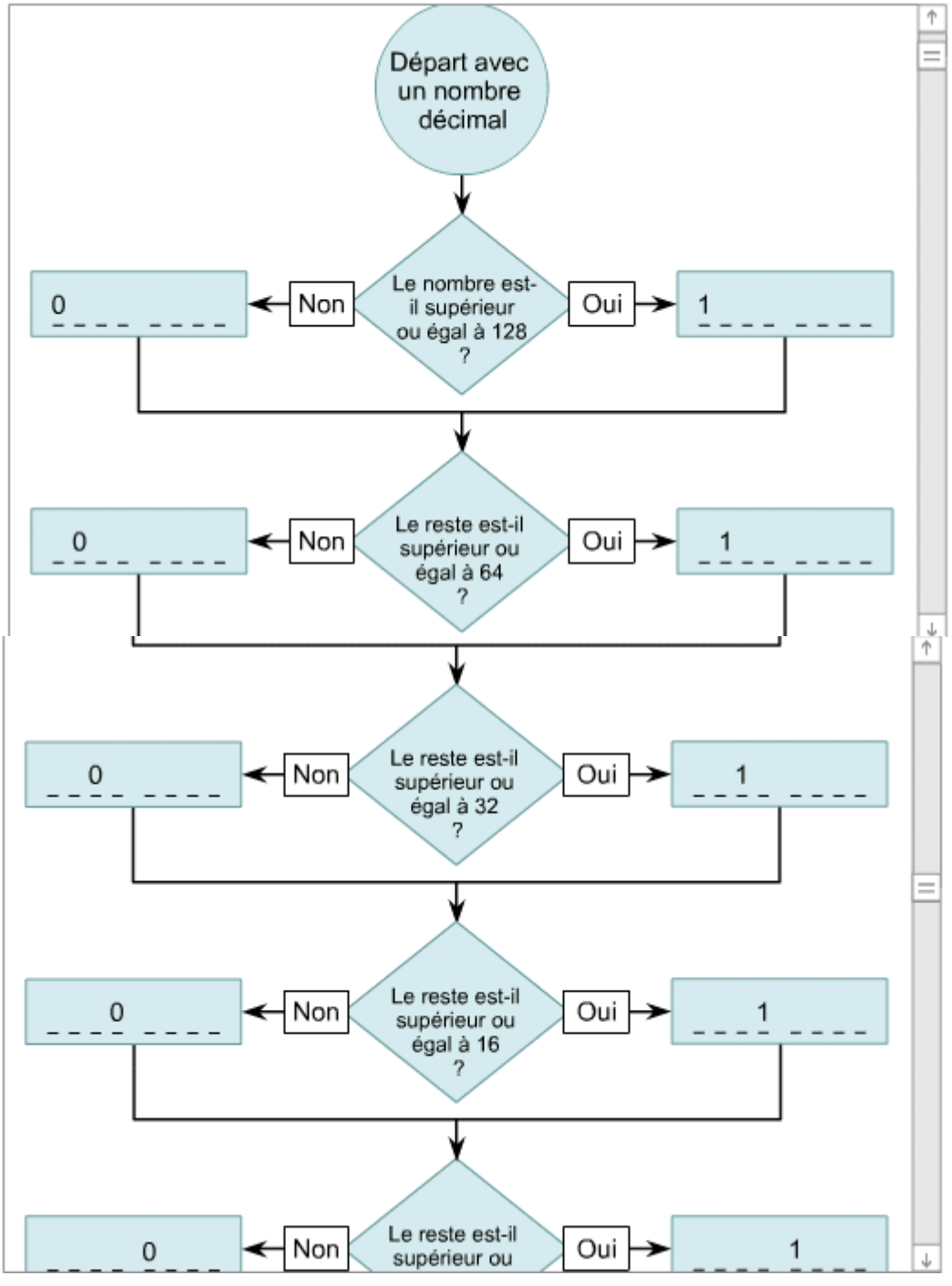
La page suivante étudie la conversion des nombres décimaux en nombres binaires.

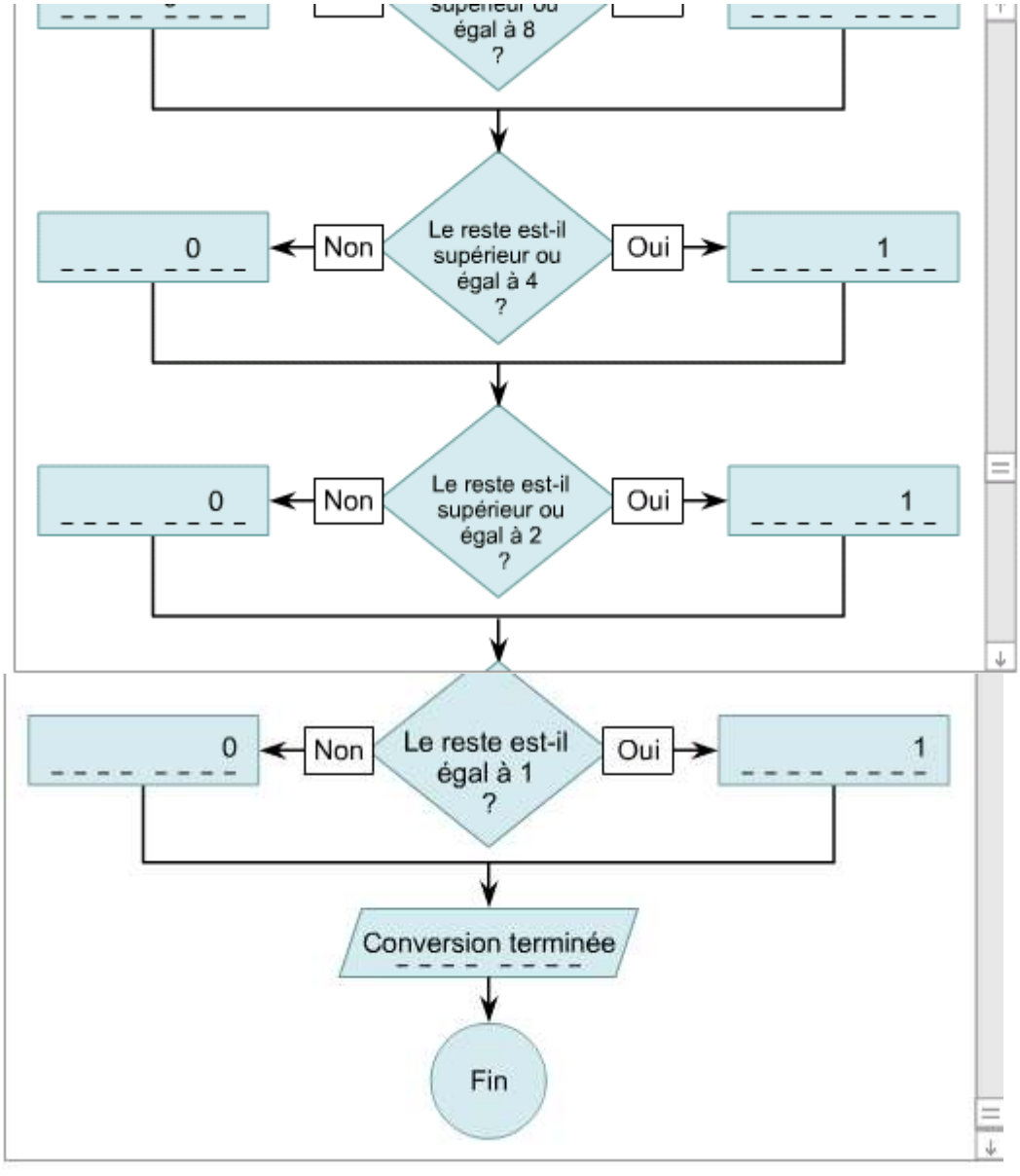
1.2 Aspects mathématiques des réseaux

1.2.5 Conversion de nombres décimaux en nombres binaires à 8 bits

Cette page porte sur la conversion de nombres décimaux en nombres binaires.

Il existe plusieurs façons de convertir les nombres décimaux en nombres binaires. L'organigramme de la figure 1


Départ avec un nombre décimal
Le nombre est-il supérieur ou égal à 128 ?
Non
Oui
0 _ _ _ _ _ _ _ _
1 _ _ _ _ _ _ _ _
Le reste est-il supérieur ou égal à 64 ?
Non
Oui
0 _ _ _ _ _ _ _ _
1 _ _ _ _ _ _ _ _
Le reste est-il supérieur ou égal à 32 ?
Non
Oui
0 _ _ _ _ _ _ _ _
1 _ _ _ _ _ _ _ _
Le reste est-il supérieur ou égal à 16 ?
Non
Oui
0 _ _ _ _ _ _ _ _
1 _ _ _ _ _ _ _ _
Le reste est-il supérieur ou
Non
Oui
0 _ _ _ _ _ _ _ _
1 _ _ _ _ _ _ _ _



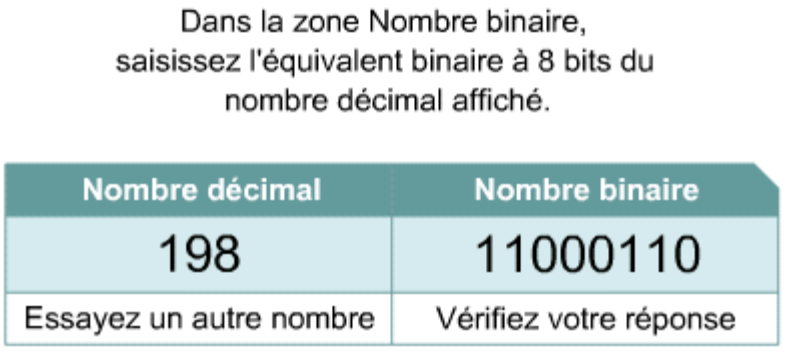
décrit une méthode parmi les différentes disponibles. Il est recommandé aux étudiants de choisir une méthode et de s'exercer à l'utiliser aussi longtemps que nécessaire pour trouver le résultat correct à chaque fois.

Exercice de conversion
Utilisez l'exemple ci-après pour convertir le nombre décimal 168 en un nombre binaire:

- 128 est inférieur à 168 donc le bit le plus à gauche du nombre binaire est 1. 168 – 128 = 40.
- 64 n'est pas inférieur ou égal à 40 donc le deuxième bit en partant de la gauche est 0.
- 32 est inférieur à 40 donc le troisième bit en partant de la gauche est 1. 40 – 32 = 8.
- 16 n'est pas inférieur ou égal à 8 donc le quatrième bit en partant de la gauche est 0.
- 8 est égal à 8 donc le cinquième bit en partant de la gauche est 1. 8 – 8 = 0. Les trois derniers bits de droite sont donc tous égaux à 0.

Cet exemple montre que le nombre décimal 168 est égal au nombre 10101000 en base 2.

Utilisez l'activité de conversion de nombres de la figure 2 pour continuer à vous entraîner.



L'activité de TP propose de s'exercer à convertir des nombres décimaux en nombres binaires.

La page suivante étudie la conversion des nombres binaires en nombres décimaux.

Activité de TP

Exercice: Conversion de nombres décimaux en nombres binaires

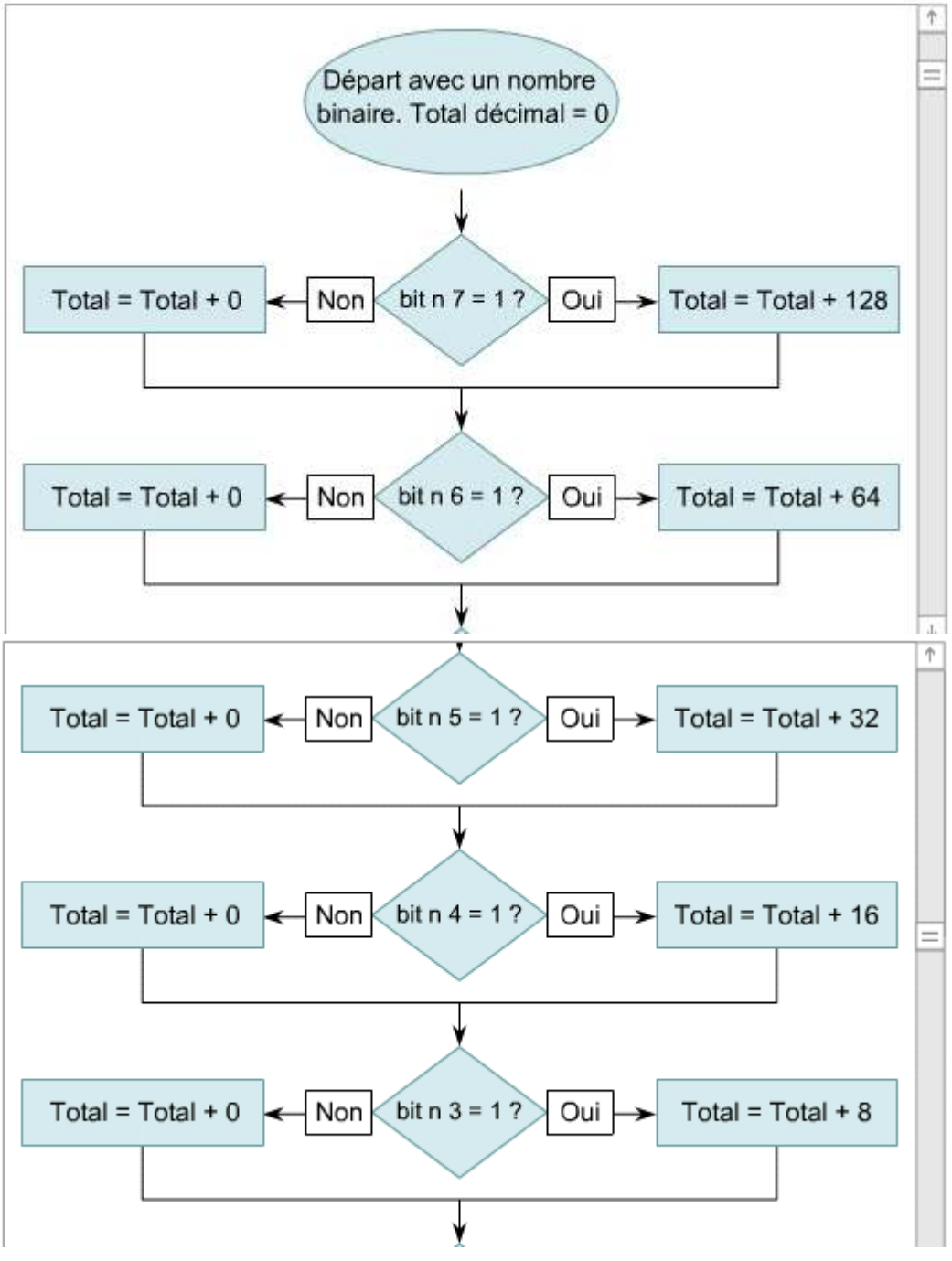
Ce TP vous permet d'apprendre et de vous entraîner à convertir des valeurs décimales en valeurs binaires.

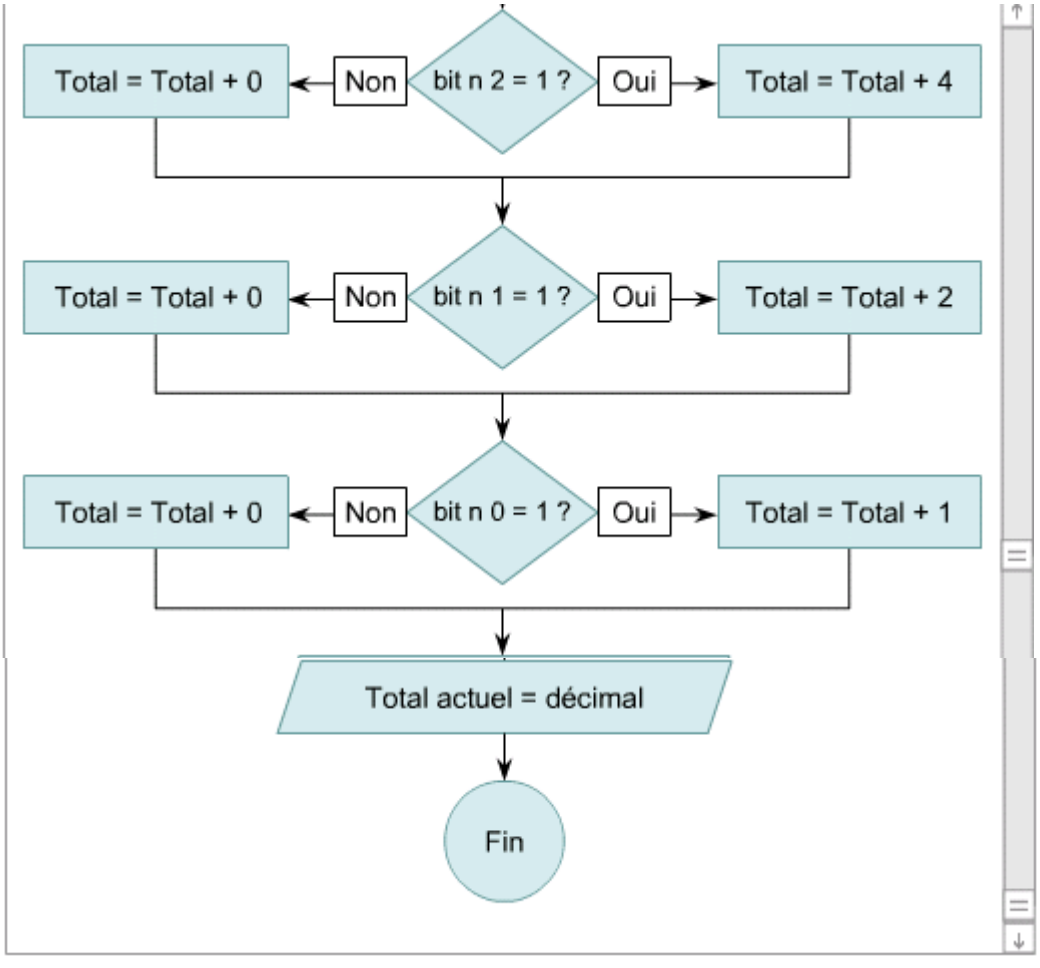
1.2 Aspects mathématiques des réseaux

1.2.6 Conversion de nombres binaires à 8 bits en nombres décimaux

Cette page porte sur la conversion de nombres binaires en nombres décimaux.

Il existe deux façons de convertir les nombres binaires en nombres décimaux. 1





L'organigramme de la figure 1 en décrit une.

Vous pouvez également multiplier chaque chiffre binaire par le nombre de base 2, élevé à la puissance correspondant au rang de ce chiffre. 2

Dans la zone Nombre décimal, saisissez
l'équivalent décimal du nombre binaire affiché.

Nombre binaire	Nombre décimal
10101101	173
Essayez un autre nombre	Vérifiez votre réponse

Correct

Voici un exemple:

Convertissez le nombre binaire 01110000 en nombre décimal.

REMARQUE:

Travaillez de droite à gauche. Gardez à l'esprit que toute valeur élevée à la puissance 0 est égale à 1.

$0 \times 2^0 = 0$

$0 \times 2^1 = 0$

$0 \times 2^2 = 0$

$0 \times 2^3 = 0$

$1 \times 2^4 = 16$

$1 \times 2^5 = 32$

$1 \times 2^6 = 64$

$+ \ 0 \times 2^7 = 0$

_____

112

L'activité de TP permet de s'exercer à convertir des nombres binaires en nombres décimaux.

La page suivante porte sur les notations entières avec points de séparation.

Activité de TP

Exercice: Conversion de nombres binaires en nombres décimaux

Ce TP vous permet d'apprendre et de vous entraîner à convertir des valeurs binaires en valeurs décimales.

1.2 Aspects mathématiques des réseaux

1.2.7 Représentation de nombres binaires à 32 bits par une notation décimale à quatre octets avec points de séparation

Cette page indique la marche à suivre pour représenter des nombres binaires par la notation décimale avec points de séparation.

A l'heure actuelle, les adresses affectées aux ordinateurs pour les identifier sur le réseau Internet sont définies par des nombres binaires de 32 bits. [1]

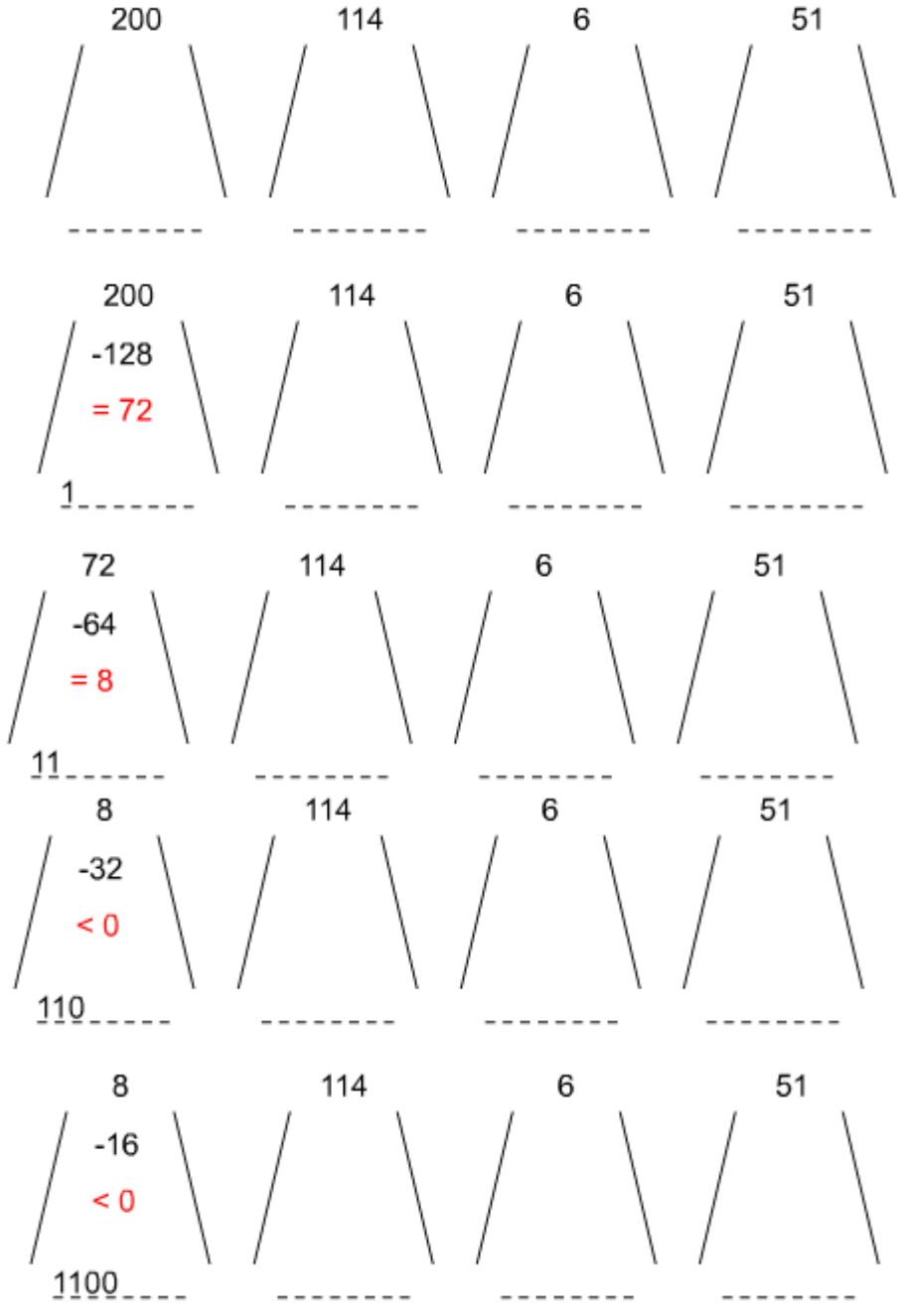
Binaire	11001000		01110010		00000110		00110011
Décimal	200	.	114	.	6	.	51
	nombre	point	nombre	point	nombre	point	nombre

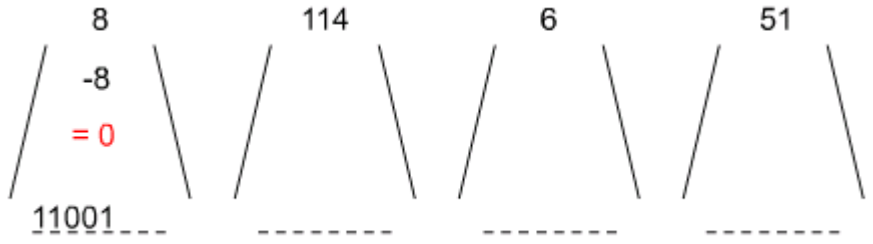
Pour faciliter l'utilisation de ces adresses, les nombres binaires de 32 bits sont décomposés en plusieurs nombres décimaux. Le nombre binaire est tout d'abord partagé en quatre groupes de huit chiffres binaires. Puis, chaque groupe de huit bits, autrement dit chaque octet, est converti en son équivalent décimal. Cette conversion est effectuée selon la méthode décrite à la page précédente.

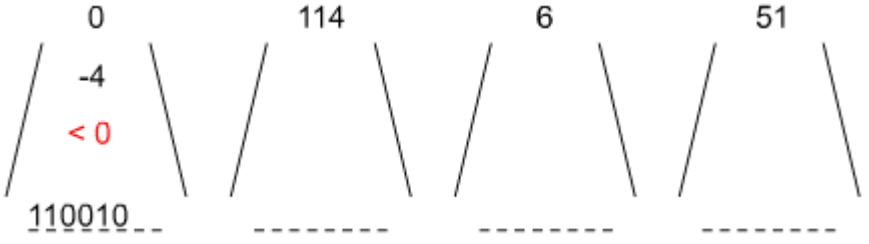
A l'écrit, le nombre binaire complet est représenté sous la forme de quatre groupes de chiffres décimaux séparés par des points. Cette règle d'écriture, appelée notation entière avec points de séparation, offre un moyen simple et concis de citer une adresse de 32 bits. Il est nécessaire de bien comprendre ce mode de représentation, employé à de nombreuses reprises dans les pages qui suivent. Pour les conversions de notation entière avec points de séparation vers nombres binaires, rappelez-vous que chaque groupe de un à trois chiffres décimaux correspond à un groupe de 8 chiffres binaires. Si le nombre décimal à convertir est inférieur à 128, vous devez ajouter au nombre binaire équivalent autant de zéros que nécessaire pour atteindre 8 bits au total.

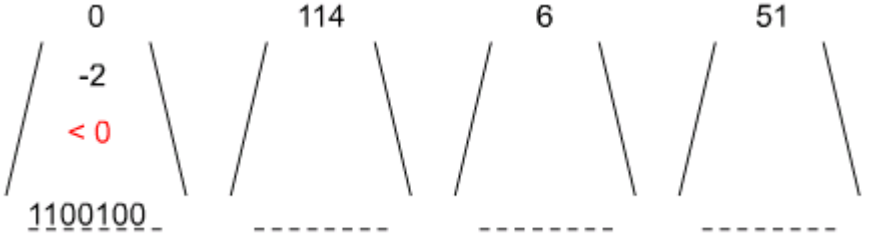
Effectuez les conversions ci-après pour vous entraîner.

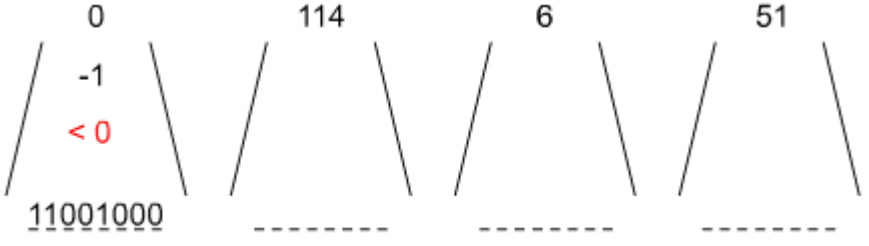
Convertissez 200.114.6.51 en son équivalent binaire de 32 bits.

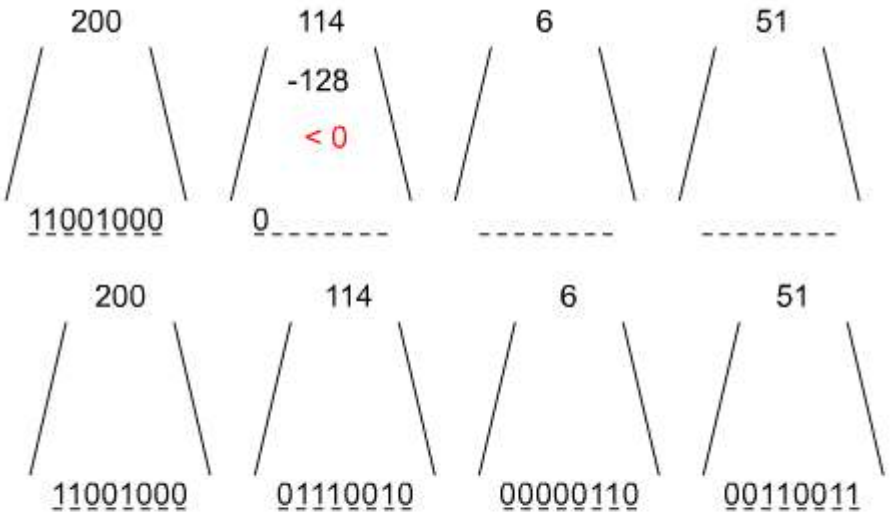



8
-8
= 0
11001
114
6
51


0
-4
< 0
110010
114
6
51


0
-2
< 0
1100100
114
6
51

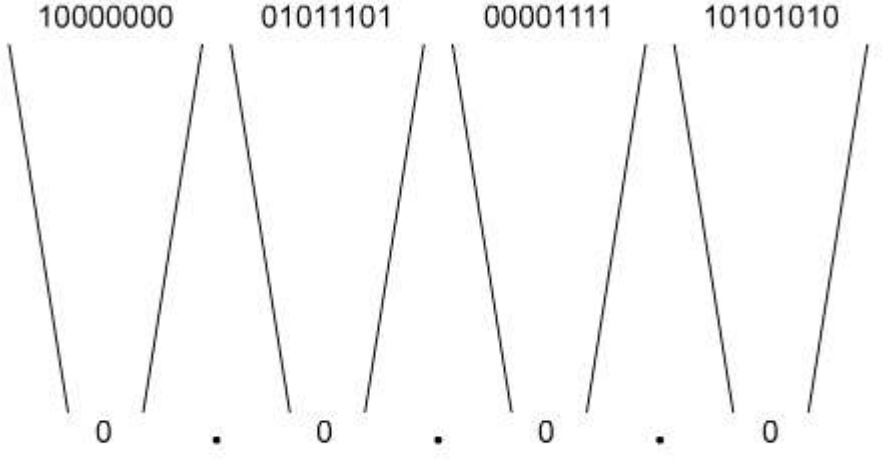

0
-1
< 0
11001000
114
6
51



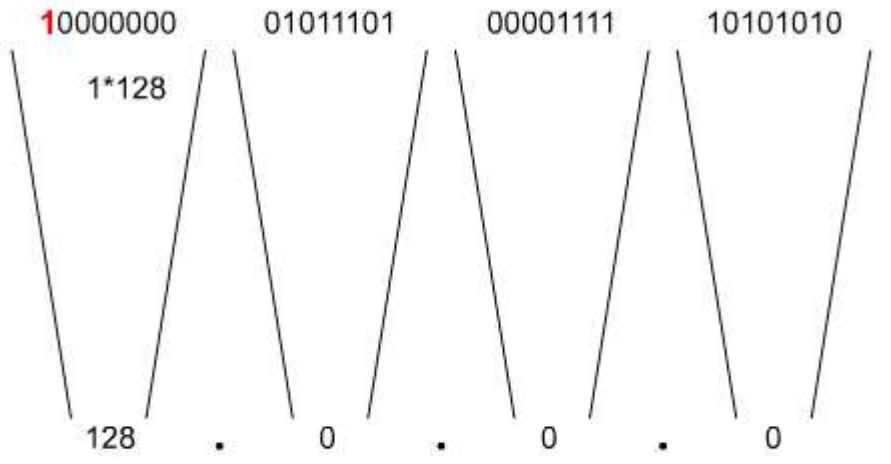
Conversion d'un nombre en notation entière avec points de séparation en un nombre binaire.

Convertissez 10000000 01011101 00001111 10101010 en notation entière avec points de séparation.

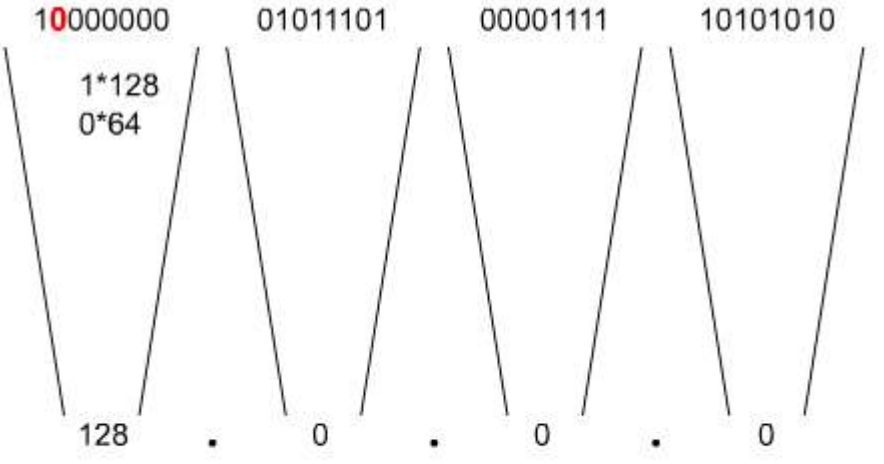
La page suivante décrit le système de numération hexadécimal. 3



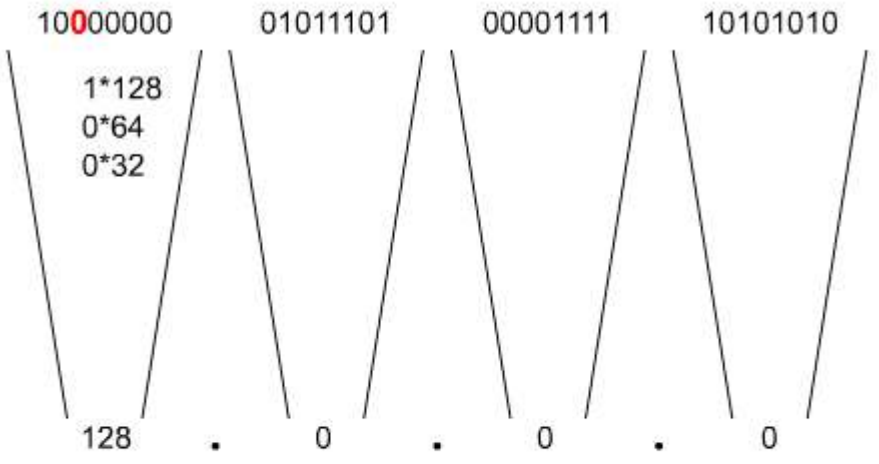
La traduction d'un nombre binaire en un nombre en notation entière avec points de séparation revient à convertir quatre fois un nombre binaire à huit bits. Chaque octet est converti séparément.



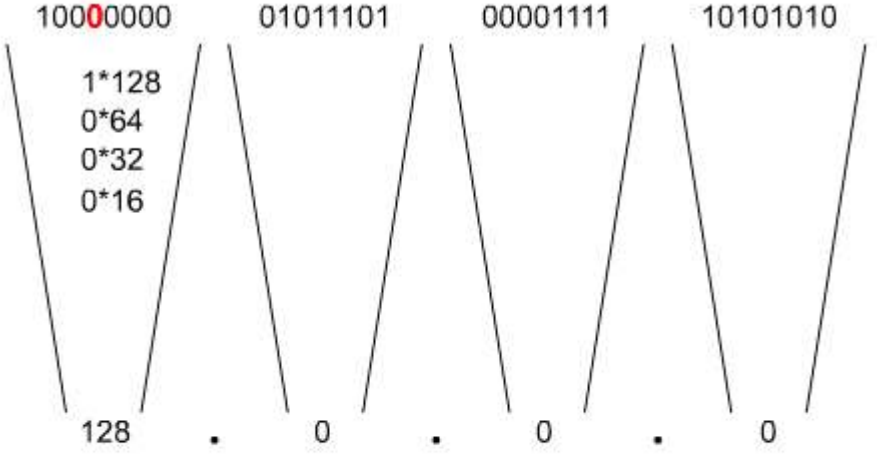
Le bit occupant le premier rang à gauche est le plus significatif (il correspond à la valeur de rang la plus élevée). Pour un nombre binaire à huit bits, le huitième rang possède la valeur décimale 128. Il convient donc d'ajouter 128 au total de conversion.



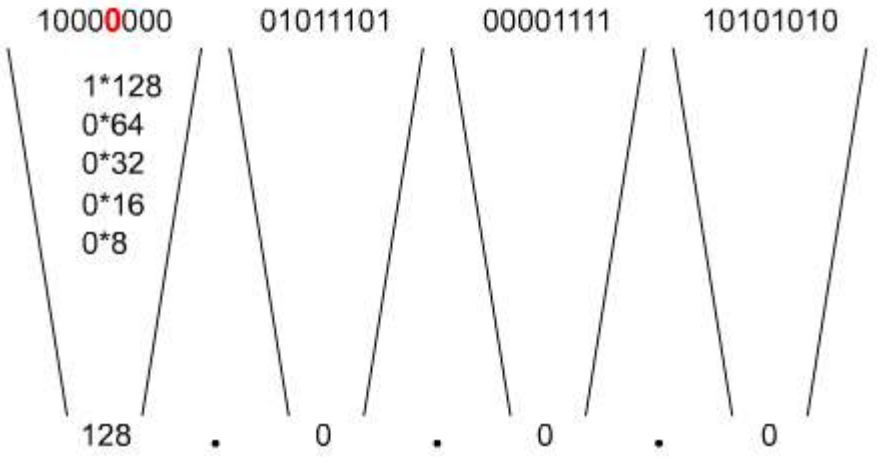
Le bit suivant à droite porte la valeur décimale 64 ; sa valeur binaire étant ici de 0, aucune valeur ne doit être inscrite pour ce rang (0*64=0). Par conséquent, le total de conversion ne change pas.



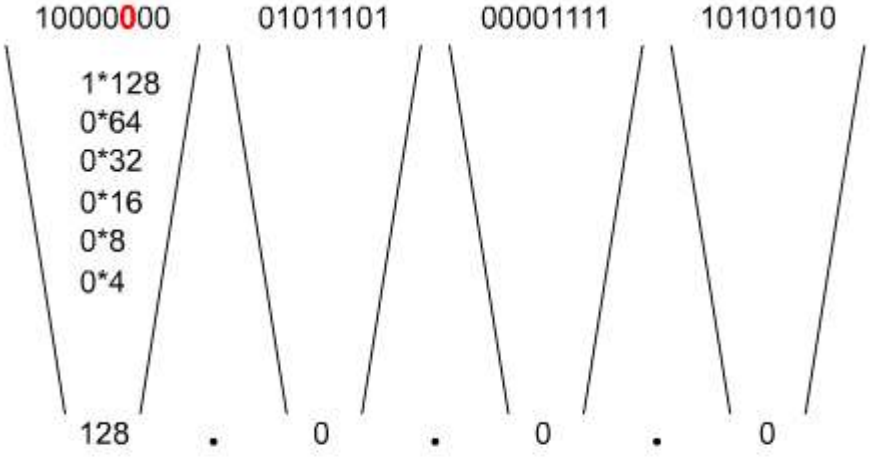
Le bit suivant à droite porte la valeur décimale 32 ; sa valeur binaire étant ici de 0, aucune valeur ne doit être inscrite pour ce rang (0*32=0). Le total de conversion ne change donc pas.



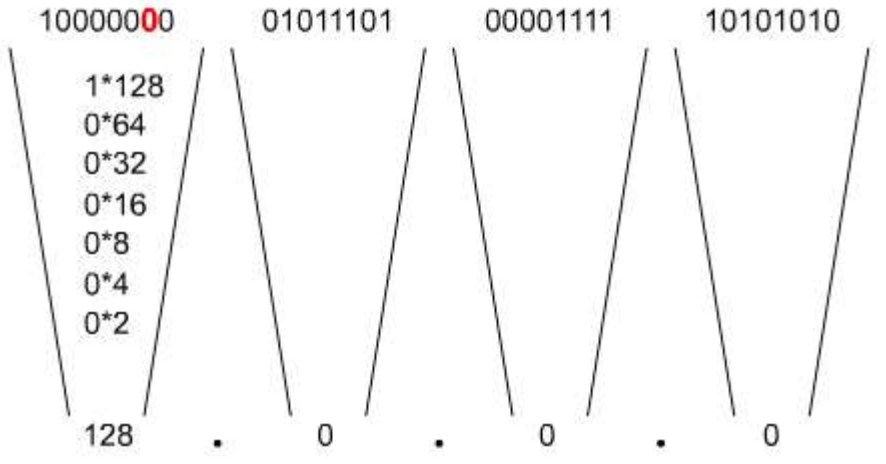
Le bit suivant à droite porte la valeur décimale 16 ; sa valeur binaire étant de 0, aucune valeur ne doit être inscrite pour ce rang (0*16=0). Le total de conversion ne change pas.



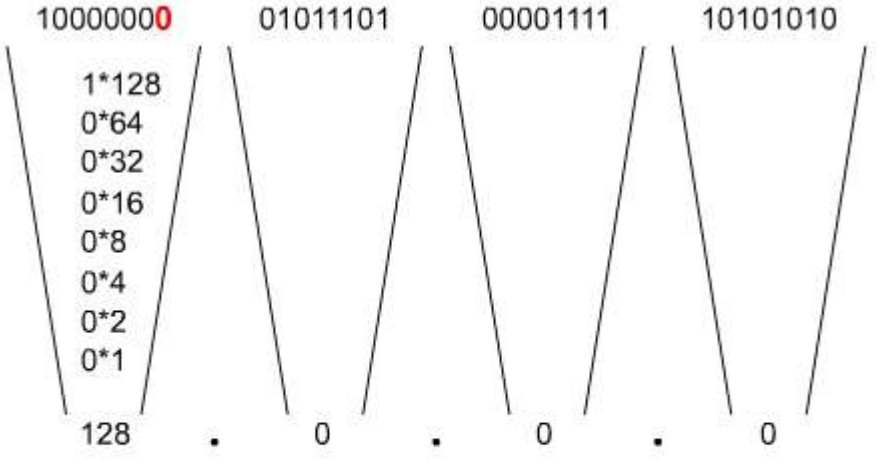
Le bit suivant à droite porte la valeur décimale 8 ; sa valeur binaire étant de 0, aucune valeur ne doit être inscrite pour ce rang (0*8=0). Le total de conversion ne change pas.



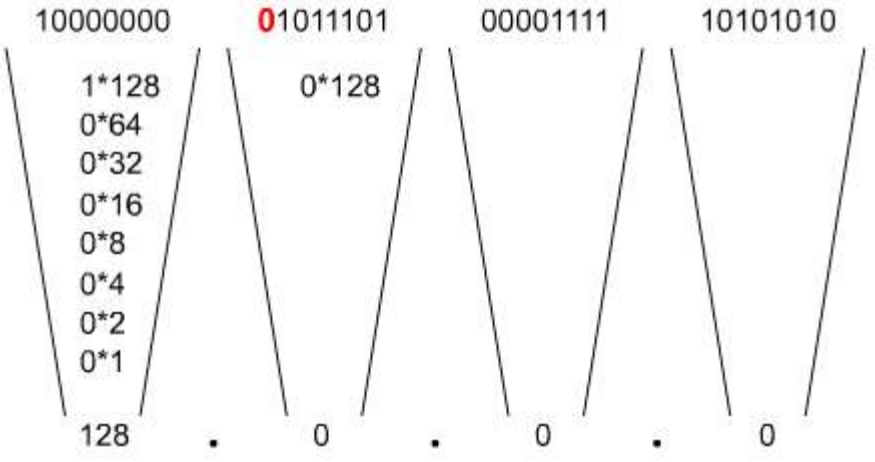
Le bit suivant à droite porte la valeur décimale 4 ; sa valeur binaire étant de 0, aucune valeur ne doit être inscrite pour ce rang (0*4=0). Le total de conversion ne change pas.



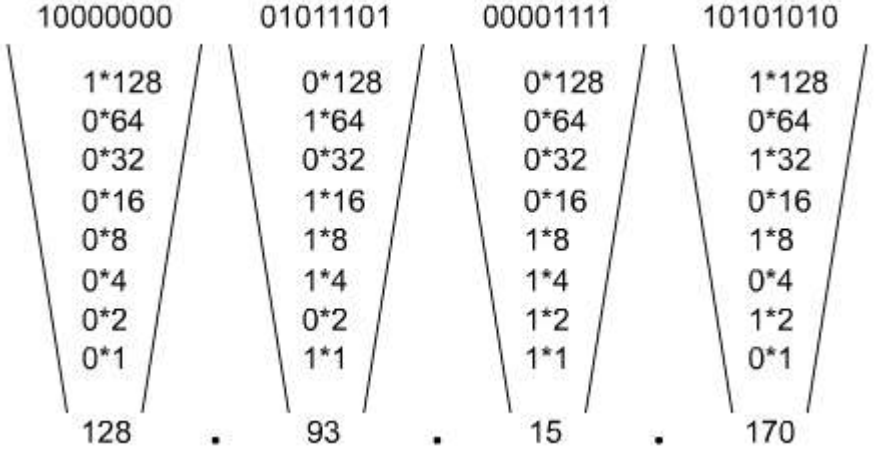
Le bit suivant à droite porte la valeur décimale 2 ; sa valeur binaire étant de 0, aucune valeur ne doit être inscrite pour ce rang (0*2=0). Le total de conversion ne change pas.



Le bit suivant à droite porte la valeur décimale 1 ; sa valeur binaire étant de 0, aucune valeur ne doit être inscrite pour ce rang (0*1=0). Le total de conversion ne change pas.



Pour le deuxième octet, procédez comme pour le premier. Lorsqu'un rang contient le chiffre binaire 1, vous devez ajouter l'équivalent décimal du rang concerné au total de conversion.



1.2 Aspects mathématiques des réseaux

1.2.8 Système hexadécimal

Cette page vous permet d'étudier le système de numération hexadécimal. Elle vous propose également d'apprendre à représenter les nombres binaires et les nombres décimaux au format hexadécimal.

Le système de numération hexadécimal ou système à base 16 est couramment utilisé pour représenter les nombres binaires sous une forme plus lisible. 1

Décimal	Binaire	Hexadécimal
0	00000000	00
1	00000001	01
2	00000010	02
3	00000011	03
4	00000100	04
5	00000101	05
6	00000110	06
7	00000111	07
8	00001000	08
9	00001001	09
10	00001010	0A
11	00001011	0B
12	00001100	0C
13	00001101	0D
14	00001110	0E
15	00001111	0F
16	00010000	10
32	00100000	20
64	01000000	40
128	10000000	80
255	11111111	FF

Les ordinateurs exécutent tous les calculs en mode binaire. Toutefois, il existe plusieurs situations dans lesquelles la valeur binaire renvoyée par un ordinateur est exprimée sous sa forme hexadécimale pour une lecture plus facile.

Ainsi, le registre de configuration des routeurs Cisco requiert souvent des conversions de valeurs hexadécimales en valeurs binaires et inversement. Les routeurs Cisco possèdent un registre de configuration d'une longueur de 16 bits. Un nombre binaire de 16 bits peut donc être représenté comme un nombre hexadécimal à quatre chiffres. Par exemple, le nombre binaire 0010000100000010 est égal à 2102 dans le système hexadécimal. Les nombres hexadécimaux ont souvent comme préfixe 0x. On écrira par exemple le nombre hexadécimal 2102 de la façon suivante : 0x2102.

Tout comme les systèmes binaire et décimal, la notation hexadécimale repose sur l'utilisation de symboles, de puissances et de rangs.

Binaire	Hexadécimal	Binaire	Hexadécimal
0000	0	1000	8
0001	1	1001	9
0010	2	1010	A
0011	3	1011	B
0100	4	1100	C
0101	5	1101	D
0110	6	1110	E
0111	7	1111	F

Les symboles utilisés sont les chiffres 0 à 9 et les lettres A à F. 3

Binaire	Hexadécimal	Décimal	Binaire	Hexadécimal	Décimal
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	A	10
0011	3	3	1011	B	11
0100	4	4	1100	C	12
0101	5	5	1101	D	13
0110	6	6	1110	E	14
0111	7	7	1111	F	15

Pour représenter n'importe quelle combinaison de quatre chiffres binaires, il suffit d'un seul symbole hexadécimal, contre un à deux symboles décimaux. La représentation d'une combinaison de huit chiffres binaires requiert deux chiffres en format hexadécimal, tandis qu'elle peut en nécessiter jusqu'à trois dans le système décimal. Étant donné qu'un symbole hexadécimal représente toujours un nombre binaire de 4 bits, la représentation hexadécimale est plus simple d'utilisation lorsque l'on travaille avec de grands nombres binaires. Ceci réduit les risques de confusion liés à la lecture de longues chaînes de nombres binaires et l'espace requis pour écrire les nombres binaires. Rappelez-vous qu'il est possible d'utiliser les caractères 0x pour désigner une valeur hexadécimale. Le nombre hexadécimal 5D peut donc s'écrire 0x5D.

Pour convertir un nombre hexadécimal en nombre binaire, il suffit de remplacer chaque chiffre hexadécimal par son équivalent binaire de quatre bits. 4

Conversion d'un nombre binaire en nombre hexadécimal

10010010001011111011111011001001
Équivaut à :
0001 0010 0100 0101 1111 0111 1101 1100 1001
Équivaut à :
1 2 4 5 F 7 D C 9
D'où :
10010010001011111011111011001001 au format binaire
= 1245F7DC9 au format hexadécimal

5

Conversion d'un nombre hexadécimal en nombre binaire

0x2102
Équivaut à :

2	1	0	2
0010	0001	0000	0010

D'où :
2102 au format hexadécimal équivaut à : 0010 0001 0000 0010 au format binaire

L'activité de TP porte sur la conversion de nombres hexadécimaux en valeurs décimales et binaires.

La page suivante traite de la logique booléenne.

Activité de TP

Exercice: Conversions hexadécimales

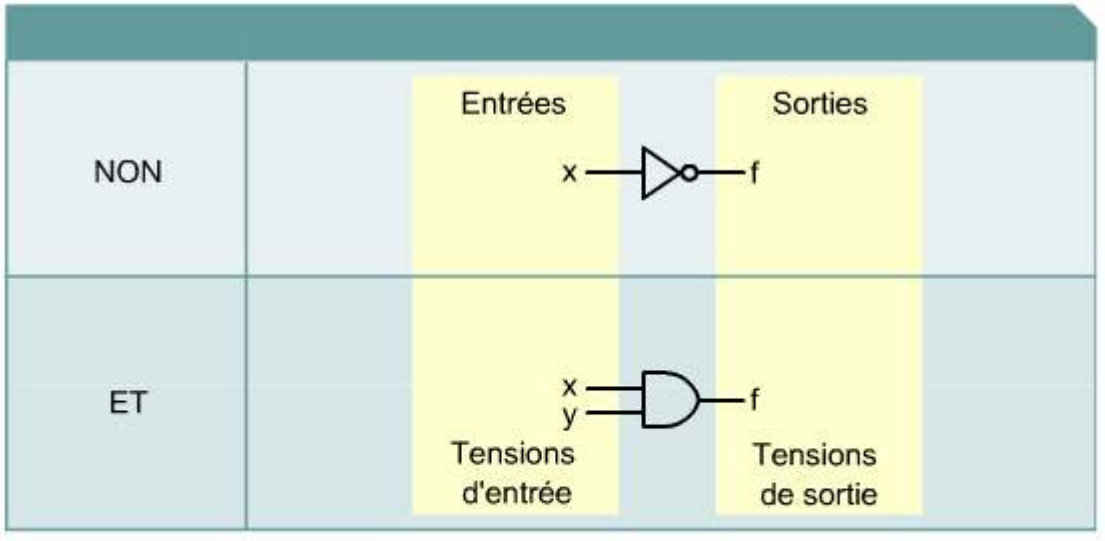
Ce TP vous permet d'apprendre à convertir des valeurs hexadécimales en valeurs décimales et binaires.

1.2 Aspects mathématiques des réseaux

1.2.9 Logique booléenne ou binaire

Cette page présente la logique booléenne et explique son fonctionnement.

La logique booléenne se rapporte aux circuits numériques acceptant une ou deux tensions électriques d'entrée. 1

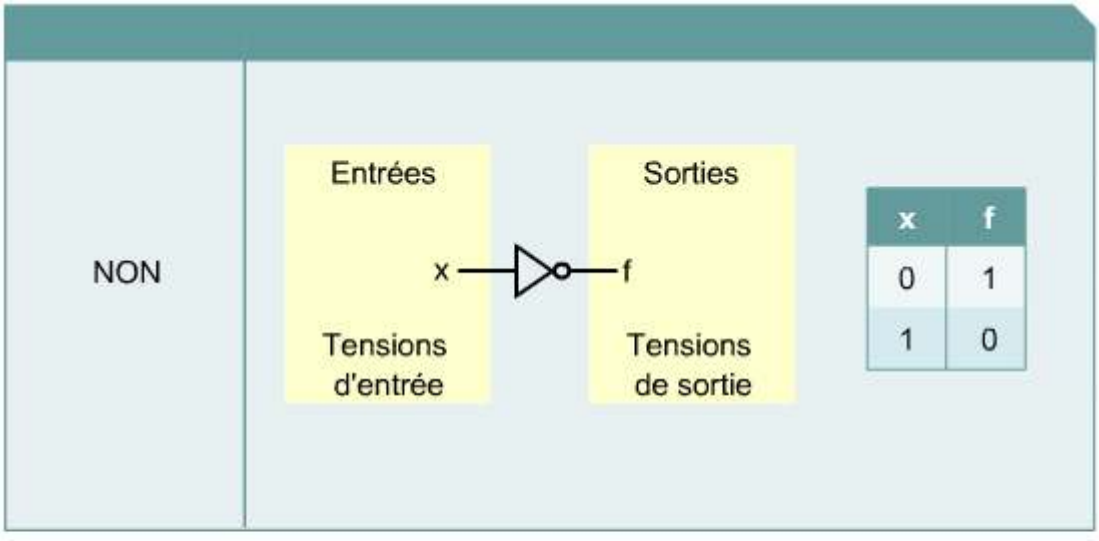


Les portes logiques acceptent une ou deux valeurs, ou tensions, d'entrée.

De la tension d'entrée dépend la tension de sortie générée. Pour les ordinateurs, les deux tensions possibles correspondent aux états En fonction et Hors fonction. A ces deux états sont associés les valeurs binaires un et zéro.

La logique booléenne est une logique binaire qui permet de comparer deux valeurs et d'effectuer un choix d'après ces valeurs. Ces choix reposent sur les opérations logiques ET, OU et NON. A l'exception de NON, les opérations booléennes remplissent la même fonction. Elles acceptent deux valeurs – 1 ou 0 – et génèrent un résultat d'après la règle de logique appliquée.

L'opération NON considère la valeur d'entrée et génère son opposé. 2

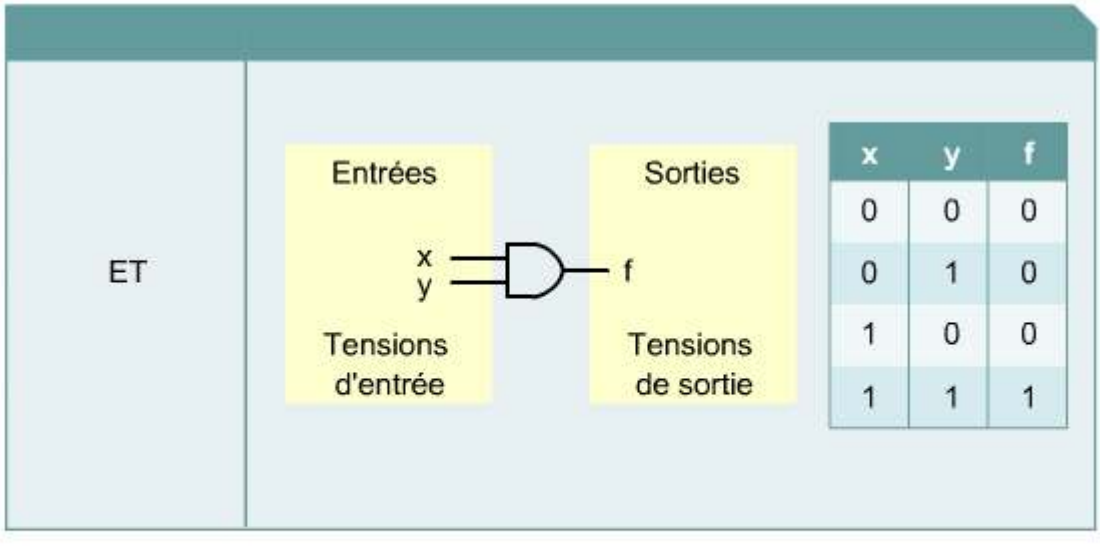


x	f
0	1
1	0

Si x égale 1 alors f égale 0. Sinon, f égale 1.

La valeur 1 donne 0 et inversement. Rappelons que les portes logiques sont des dispositifs électroniques conçus spécialement pour exécuter une fonction particulière. Pour la fonction NON, la règle logique appliquée consiste à générer, quelle que soit la valeur d'entrée, la valeur opposée en sortie.

L'opération ET compare deux valeurs d'entrée. Si les deux valeurs sont égales à 1, la porte logique génère la valeur de sortie 1. 3

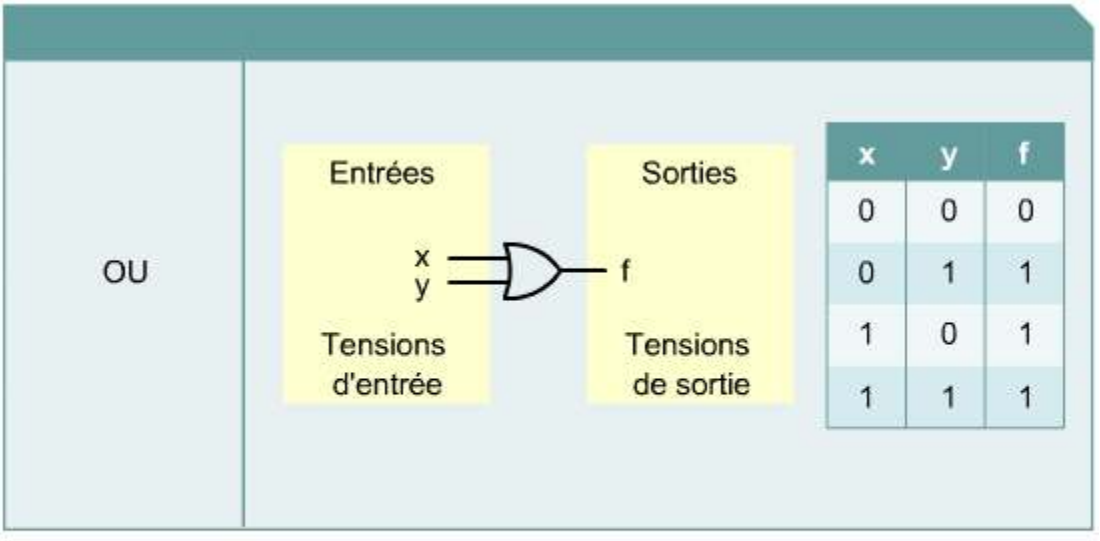


x	y	f
0	0	0
0	1	0
1	0	0
1	1	1

Si x égale 1 et y égale 1 alors f égale 1. Sinon, f égale 0.

Sinon, elle renvoie la valeur 0. Il existe quatre combinaisons de valeurs d'entrée ; trois d'entre elles donnent 0 comme valeur de sortie de 0 et une seule génère la valeur 1.

L'opération OU prend également en compte deux valeurs d'entrée. 4



Si x égale 1 ou y égale 1 alors f égale 1. Sinon, f égale 0.

Si l'une d'elles au moins est égale à 1, alors la valeur de sortie est de 1. Comme pour l'opération ET, quatre combinaisons de valeurs d'entrée sont possibles. Trois de ces combinaisons donnent une valeur de sortie de 1, tandis que la quatrième génère un 0.

Dans un réseau, deux types d'opérations font appel à la logique booléenne : la création de masques de sous-réseau et de masques génériques, qui permettent de filtrer des adresses. Utilisées pour identifier les équipements du réseau, les adresses peuvent être regroupées en plusieurs sous-ensembles ou contrôlées par des outils réseau différents. Toutes ces fonctions font l'objet d'une présentation détaillée dans la suite du cursus.

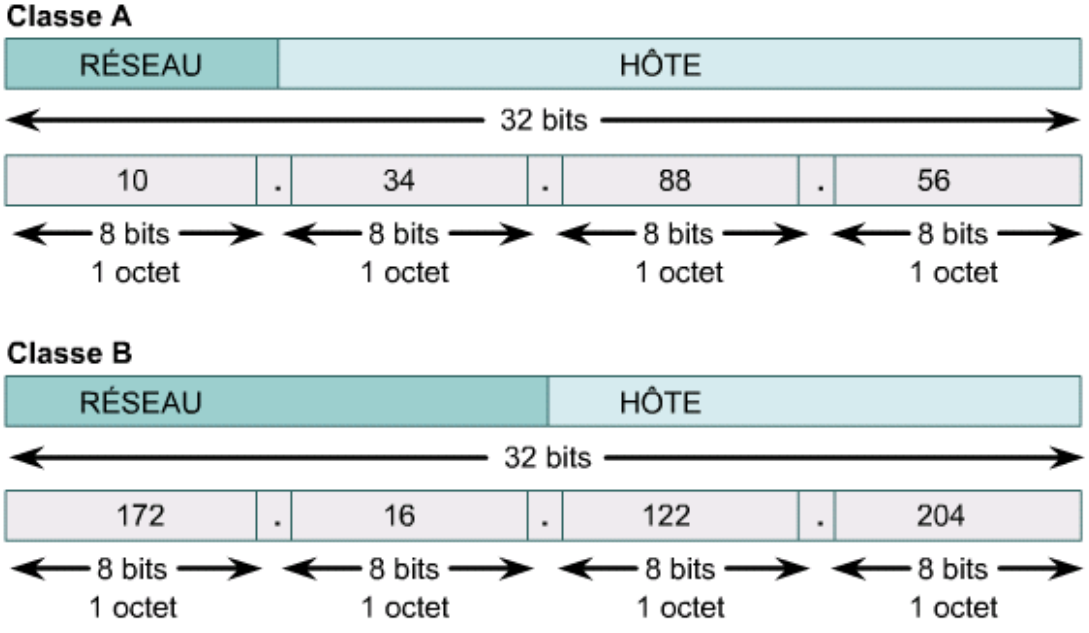
La page suivante décrit l'utilisation des masques de réseau.

1.2 Aspects mathématiques des réseaux

1.2.10 Adresses IP et masques de réseau

Cette page décrit la relation existant entre les adresses IP et les masques de réseau.

Dans l'adresse IP affectée à un ordinateur inclus dans un réseau, plusieurs bits situés à gauche du numéro IP de 32 bits servent à représenter le réseau. Le nombre de bits réservés à cet effet dépend de la classe de l'adresse. 1



Les bits restants de l'adresse IP à 32 bits identifient un ordinateur particulier sur le réseau. Le terme « hôte » est employé pour désigner un ordinateur. L'adresse IP de chaque ordinateur se compose donc d'une partie réseau et d'une partie hôte.

Pour définir la décomposition de l'adresse IP à 32 bits d'un ordinateur, un second numéro de 32 bits, appelé masque de sous-réseau, est utilisé. Ce masque fournit un guide pour l'interprétation de l'adresse IP. Il indique combien de bits sont réservés à l'identification du réseau dont fait partie l'ordinateur. La partie gauche du masque de sous-réseau est formée d'une série de 1 successifs. Tous les bits du masque qui correspondent à l'adresse du réseau ont la valeur 1, tandis que le reste du masque comporte des zéros. Les bits du masque de sous-réseau qui portent la valeur 0 identifient l'hôte.

Les exemples ci-après sont des masques de sous-réseau.

11111111000000000000000000000000 ou, en notation entière avec points de séparation, 255.0.0.0

11111111111111110000000000000000 ou, en notation entière avec points de séparation, 255.255.0.0

Dans le premier exemple, les huit premiers bits en partant de la gauche représentent la partie réseau de l'adresse et les 24 autres bits, la partie hôte. Dans le second exemple, les 16 premiers bits représentent la partie réseau de l'adresse et les 16 autres bits, la partie hôte.

L'adresse IP 10.34.23.134 correspond, en représentation binaire, à :

00001010.00100010.00010111.10000110

L'opération booléenne ET appliquée à l'adresse IP 10.34.23.134 et au masque de sous-réseau 255.0.0.0 permet d'obtenir l'adresse du réseau dont fait partie l'hôte:

00001010.00100010.00010111.10000110
11111111.00000000.00000000.00000000
00001010.00000000.00000000.00000000

Après conversion en notation entière avec points de séparation, cette adresse devient 10.0.0.0 et représente la partie réseau de l'adresse IP lorsque le masque 255.0.0.0 est utilisé.

L'opération booléenne ET appliquée à l'adresse IP 10.34.23.134 et au masque de sous-réseau 255.255.0.0 permet d'obtenir l'adresse du réseau dont fait partie l'hôte:

00001010.00100010.00010111.10000110
11111111.11111111.00000000.00000000
00001010.00100010.00000000.00000000

Après conversion en notation entière avec points de séparation, cette adresse devient 10.34.0.0 et représente la partie réseau de l'adresse IP lorsque le masque 255.255.0.0 est utilisé.

Ceci illustre brièvement la signification d'un masque de sous-réseau pour une adresse IP. La réalisation d'activités supplémentaires concernant les adresses IP permettra de comprendre plus précisément l'utilité de tels masques. Au stade actuel, assurez-vous seulement de comprendre la notion de masque.

Cette leçon est terminée. La page suivante reprend les points importants de ce module.

Résumé

- Les trois éléments requis pour une connexion à Internet sont : une connexion physique, une connexion logique et un navigateur Web.
- Les ordinateurs reconnaissent et traitent les données au moyen d'un système de numération binaire.
- Le système de numération le plus courant est le système décimal.
- Le système de numération hexadécimal permettant de représenter des nombres binaires sous une forme plus lisible, il est important de connaître ce système lorsque l'on utilise des ordinateurs.

Cette page récapitule les thèmes abordés tout au long du module.

La connexion à un réseau d'ordinateurs se compose d'une connexion physique, d'une connexion logique et des applications requises pour interpréter les données et afficher les informations. Pour établir la connexion physique et en assurer la maintenance, il est nécessaire de connaître les composants et les périphériques des PC. La connectivité à Internet nécessite un adaptateur, qui peut être un modem ou une carte réseau.

Apparus au début des années 1960, les modems assuraient alors la connectivité à un ordinateur central. Depuis, les méthodes d'accès ont évolué pour offrir aujourd'hui des services garantissant une connexion permanente à haut débit.

La connexion logique, quant à elle, utilise des normes, plus précisément appelées protocoles, parmi lesquels les protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*) sont les plus largement utilisés. Différents utilitaires du système d'exploitation permettent de configurer la connexion TCP/IP sur une station de travail. L'utilitaire ping sert à tester la connectivité du réseau.

Un navigateur Web est un logiciel installé sur un PC pour permettre l'accès aux pages Web locales et aux sites Internet. Outre le navigateur, des modules d'extension sont parfois nécessaires : ces applications fonctionnent conjointement avec le navigateur pour lancer le programme permettant d'afficher certains fichiers propriétaires ou spéciaux.

Les ordinateurs reconnaissent et traitent les données à l'aide du système de numération binaire (base 2). Souvent, les valeurs binaires générées par un ordinateur sont exprimées au format hexadécimal pour un meilleur confort de lecture. La capacité à convertir des nombres décimaux en nombres binaires s'avère importante, notamment pour représenter des adresses IP en notation entière avec points de séparation par des adresses au format binaire, lisible par l'ordinateur. La conversion de nombres hexadécimaux en nombres binaires et inversement est une opération courante dans le registre de configuration des routeurs Cisco.

La logique booléenne est une logique binaire qui permet de comparer deux valeurs et d'effectuer un choix d'après ces valeurs. Dans un réseau, deux types d'opérations font appel à la logique booléenne : la création de masques de sous-réseau et de masques génériques.

Les adresses binaires à 32 bits utilisées sur le réseau Internet sont appelées adresses IP (*Internet Protocol*).

2-Notions de base sur les réseaux

Vue d'ensemble

Les décisions relatives à la bande passante comptent parmi les aspects les plus importants de la conception d'un réseau. Ce module expose l'importance de la bande passante et explique la façon de la mesurer.

On se sert de modèles en couches pour décrire les différentes fonctions de réseau. Le présent module décrit les deux modèles les plus importants, à savoir le modèle OSI (*Open System Interconnection*) et le modèle TCP/IP (*Transmission Control Protocol/Internet Protocol*). Il présente également les différences et les similitudes entre les deux modèles.

Il retrace également un bref historique des réseaux. Les étudiants découvriront les équipements de réseau et les différents types de dispositions physiques et logiques. Ce module décrit et compare également les réseaux LAN, MAN, WAN, SAN et les VPN.

Il porte sur certains des objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811.

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de produits Cisco • Sélection de services WAN répondant aux besoins des clients	• Mise en œuvre d'un LAN	• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	• Description des communications réseau à l'aide des modèles en couche • Évaluation du processus de communication TCP/IP et de ses protocoles associés • Évaluation des principales caractéristiques des réseaux WAN • Comparaison des principales caractéristiques des environnements LAN

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Mise en œuvre d'un LAN	• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	• Évaluation des caractéristiques des environnements LAN

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Description et installation du matériel et des logiciels requis pour pouvoir communiquer via un réseau	• Description des propriétés physiques, électriques et mécaniques ainsi que des normes associées aux médias optique, sans fil et cuivre utilisés dans les réseaux • Description des topologies et des problèmes physiques liés au câblage des LAN les plus courants • Identification des principales caractéristiques des technologies et des configurations WAN (Wide Area Networking) courantes, et différences par rapport aux technologies LAN les plus répandues • Définition et description de la structure des réseaux informatiques et des technologies associées • Description du matériel et des logiciels requis pour pouvoir communiquer via un réseau

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
2.1	Terminologie de réseau
2.2	Bande passante
2.3	Modèles de réseau

- Expliquer l'importance de la bande passante dans le réseau
- Décrire la bande passante en utilisant une analogie
- Identifier les unités de mesure de bande passante, c'est-à-dire bits/s, kbits/s, Mbits/s et Gbits/s
- Expliquer la différence entre bande passante et débit
- Calculer la vitesse de transfert de données
- Expliquer pourquoi les modèles en couches sont utilisés pour décrire la communication des données
- Expliquer le développement du modèle OSI
- Dresser la liste des avantages d'une approche en couches
- Identifier chacune des sept couches du modèle OSI
- Identifier les quatre couches du modèle TCP/IP
- Décrire les similitudes et les différences entre les deux modèles
- Retracer brièvement l'historique des réseaux
- Identifier les équipements utilisés dans les réseaux
- Comprendre le rôle des protocoles dans les réseaux
- Définir les réseaux LAN, WAN, MAN et SAN
- Expliquer les réseaux VPN et leurs avantages
- Indiquer les différences entre les intranets et les extranets

2.1 Terminologie de réseau

2.1.1 Réseaux de données

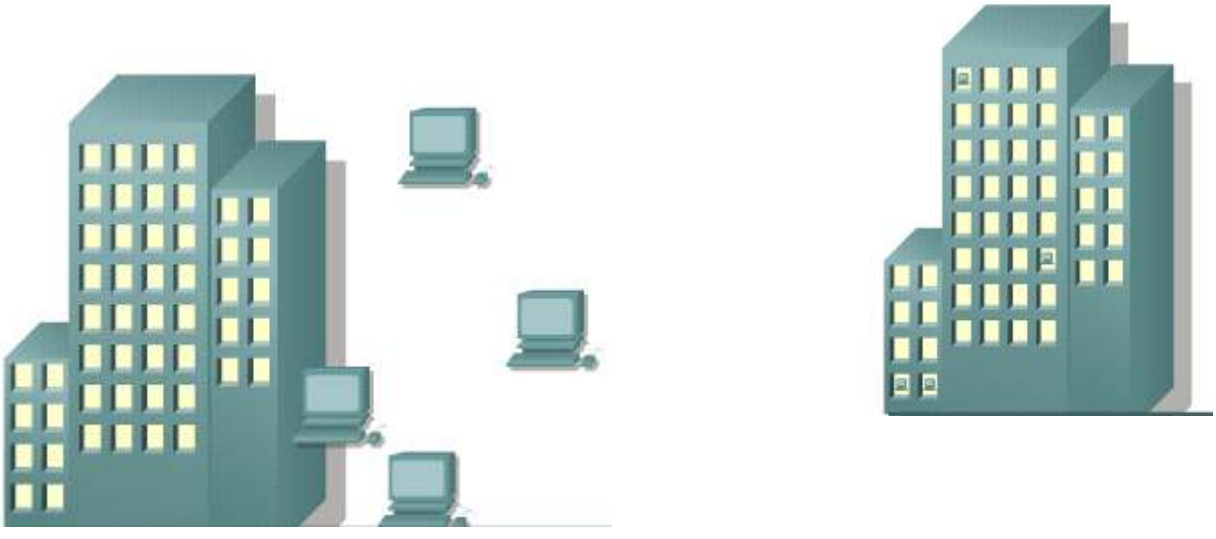
Cette page traite de l'évolution des réseaux de données.

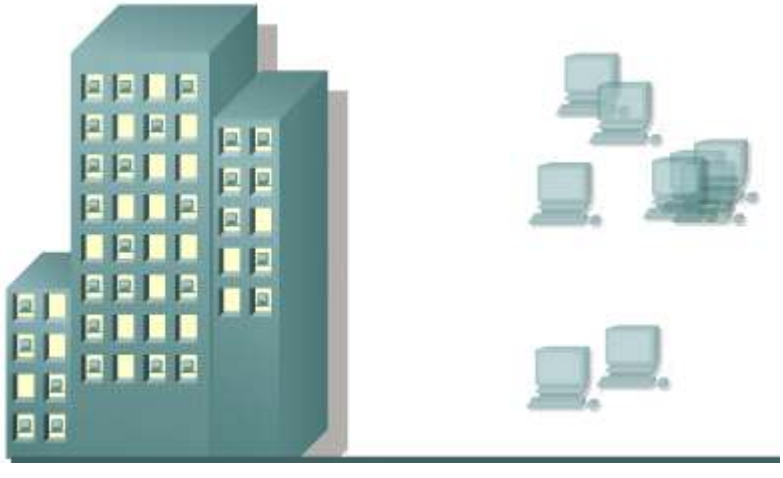
Ce sont les applications d'entreprise écrites pour les micro-ordinateurs qui ont conduit au développement des réseaux de données. 1

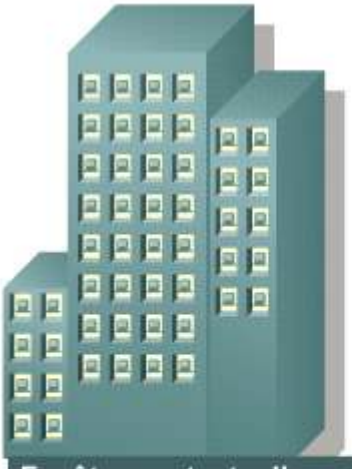


Fenêtre contextuelle

Les entreprises ont mis du temps à adopter les PC. L'apparition de Lotus 1-2-3 et d'autres applications conçues pour l'entreprise a favorisé la croissance rapide de l'industrie des ordinateurs personnels ou PC.







Fenêtre contextuelle

Les entreprises ont mis du temps à adopter les PC. L'apparition de Lotus 1-2-3 et d'autres applications conçues pour l'entreprise a favorisé la croissance rapide de l'industrie des ordinateurs personnels ou PC.

Les micro-ordinateurs n'étant pas interconnectés, il n'existait alors aucun moyen efficace de partager les données. 2



Fenêtre contextuelle

Autrefois, les entreprises investissaient dans des ordinateurs qu'elles utilisaient comme des unités indépendantes, parfois reliées à une imprimante. Pour imprimer des documents, les employés qui n'avaient pas d'imprimante devaient copier leurs fichiers sur disquette et transporter la disquette pour pouvoir imprimer à partir d'un poste différent possédant une imprimante. Cette version plutôt grossière d'un réseau était appelée " Réseau disquettes ".

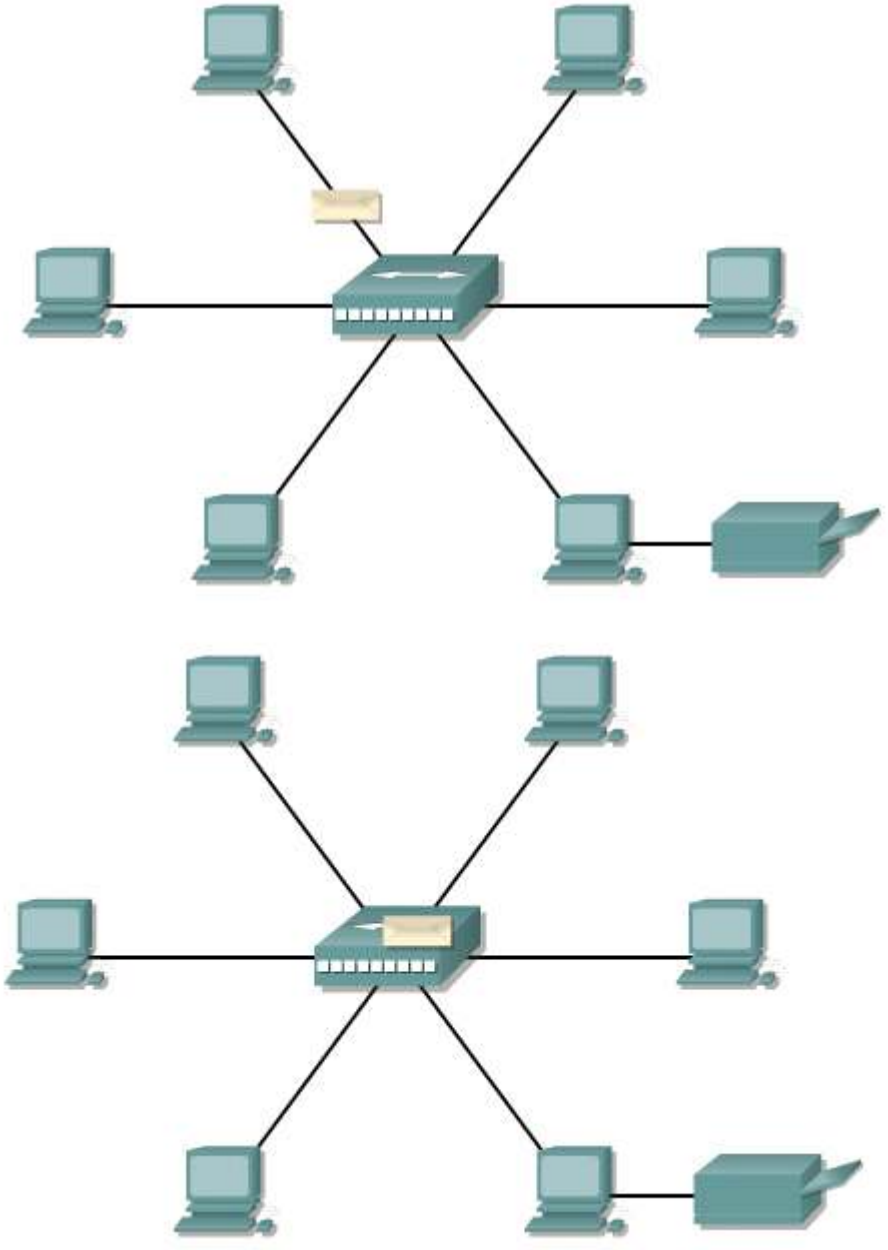


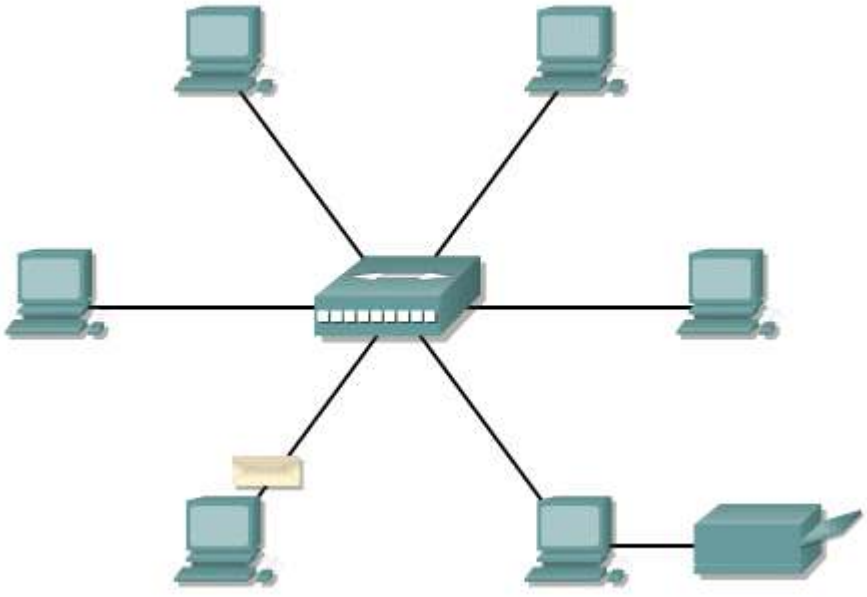
Pour les entreprises, il n'était ni efficace ni rentable d'utiliser des disquettes pour partager des données. Le «réseau disquettes» multipliait les copies des données. Chaque fois qu'un fichier était modifié, il fallait le partager à nouveau avec toutes les autres personnes qui en avaient besoin. Si deux personnes modifiaient le fichier puis essayaient de le partager, l'un des ensembles de modifications était perdu. Il fallait aux entreprises une solution qui apporte des réponses aux trois problèmes suivants:

- Comment éviter la duplication de l'équipement et des ressources
- Comment communiquer de manière efficace
- Comment mettre en place et gérer un réseau

Les entreprises ont vite réalisé que la mise en réseau des ordinateurs pouvait augmenter leur productivité et leur faire économiser de l'argent. Les réseaux furent implantés partout, favorisés par l'éclosion rapide de nouvelles technologies et de nouveaux produits de réseau. À ses débuts, le développement des réseaux était quelque peu désorganisé. Les technologies de réseau créées au milieu des années 80 étaient basées sur des implémentations matérielles et logicielles diversifiées. À cette époque, chaque société qui créait des matériels et des logiciels de réseau utilisait ses propres normes. Ces normes individuelles permettaient de contrer la concurrence. En conséquence, la plupart des technologies réseau étaient incompatibles entre elles. Il devenait donc de plus en plus difficile de faire communiquer les réseaux qui utilisaient des spécifications différentes. Il fallait souvent remplacer des équipements de réseau pour pouvoir implémenter de nouvelles technologies.

L'une des premières solutions a été l'élaboration des normes de réseau local (LAN). 3



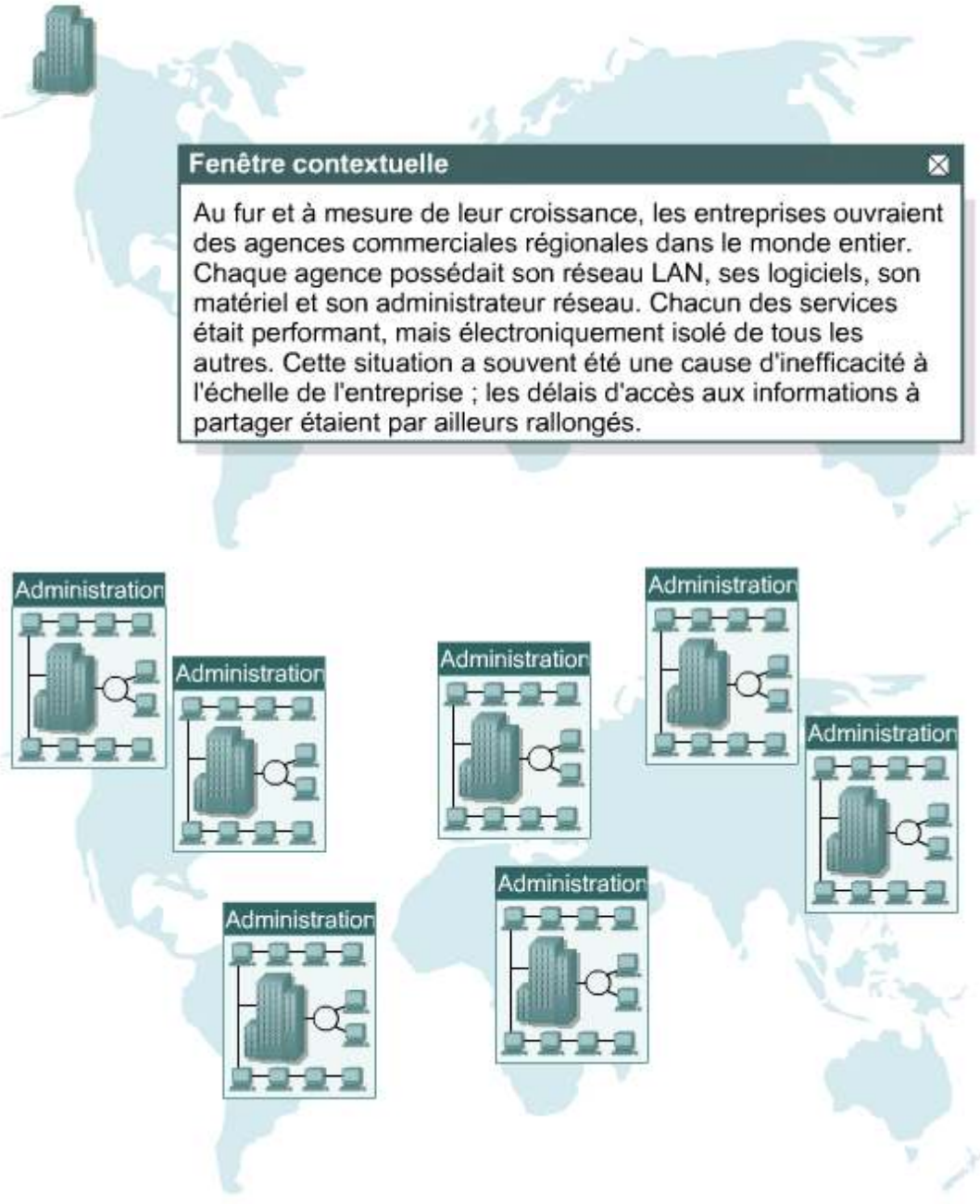


Fenêtre contextuelle

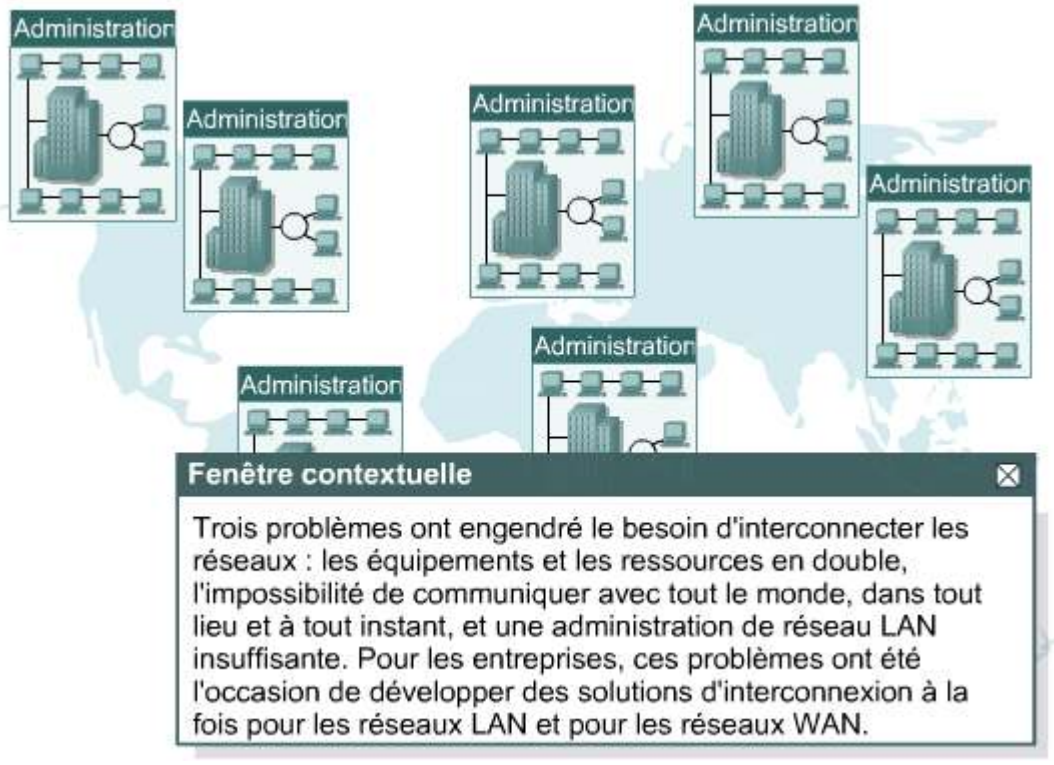
Avec la croissance de l'entreprise, les inconvénients du " réseau disquettes " sont rapidement devenus évidents. Les entreprises ont alors investi dans des réseaux locaux ou LAN (Local Area Network). Grâce à la technologie des LAN, les utilisateurs des différents services d'une entreprise ont été en mesure de transférer rapidement des fichiers par voie électronique sur le réseau. Les imprimantes autonomes ont été remplacées par des imprimantes réseau à haut débit, partagées par des services entiers. Malgré cela, le " réseau disquettes " demeurait le seul procédé possible pour partager des fichiers avec des personnes appartenant à un autre service ou un autre LAN.

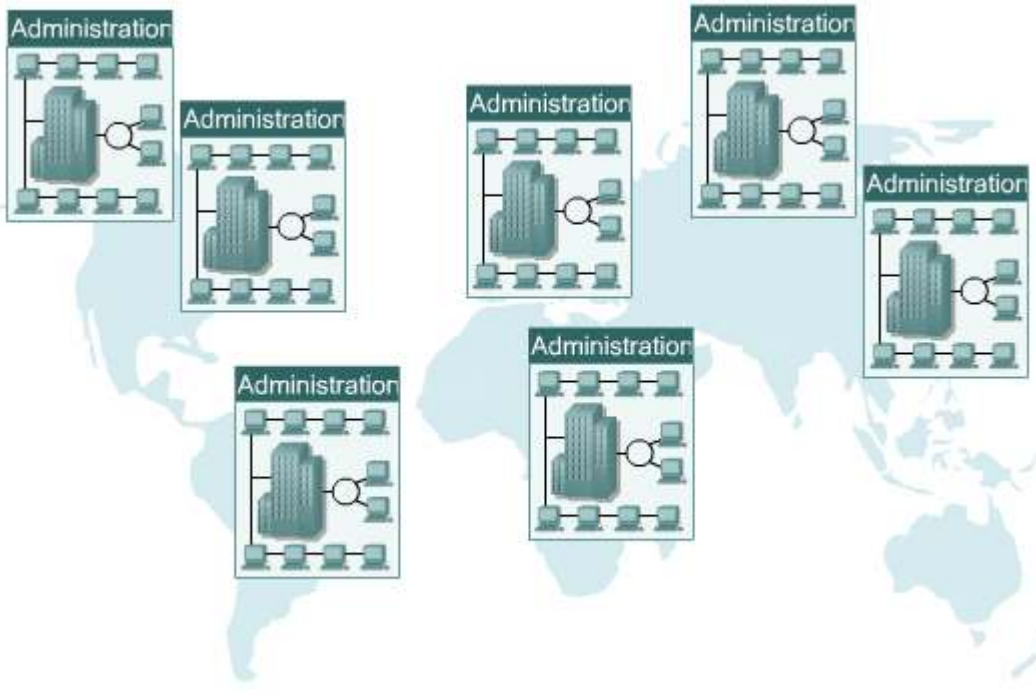
Les normes de réseau local ont établi un ensemble de directives ouvert sur lequel les sociétés se sont basées pour créer des matériels et des logiciels de réseau. De ce fait, les équipements des différentes sociétés sont devenus compatibles. Un autre effet positif a été la stabilité dans les implémentations de réseau local.

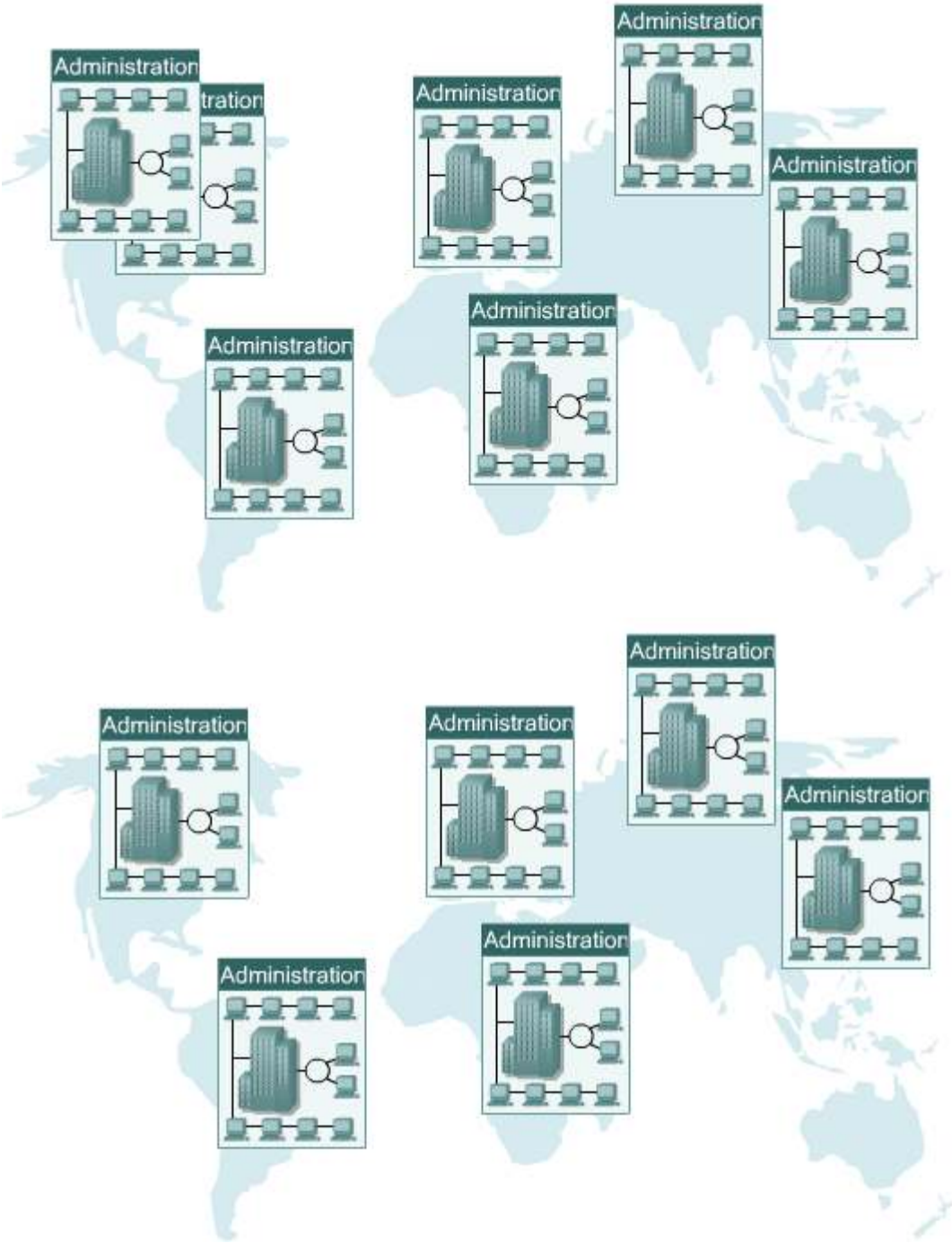
Dans un système de réseau local, chaque service de l'entreprise peut être comparé à un îlot électronique. Lorsque l'utilisation des ordinateurs dans les entreprises s'est généralisée, les réseaux locaux se sont vite avérés insuffisants. 4

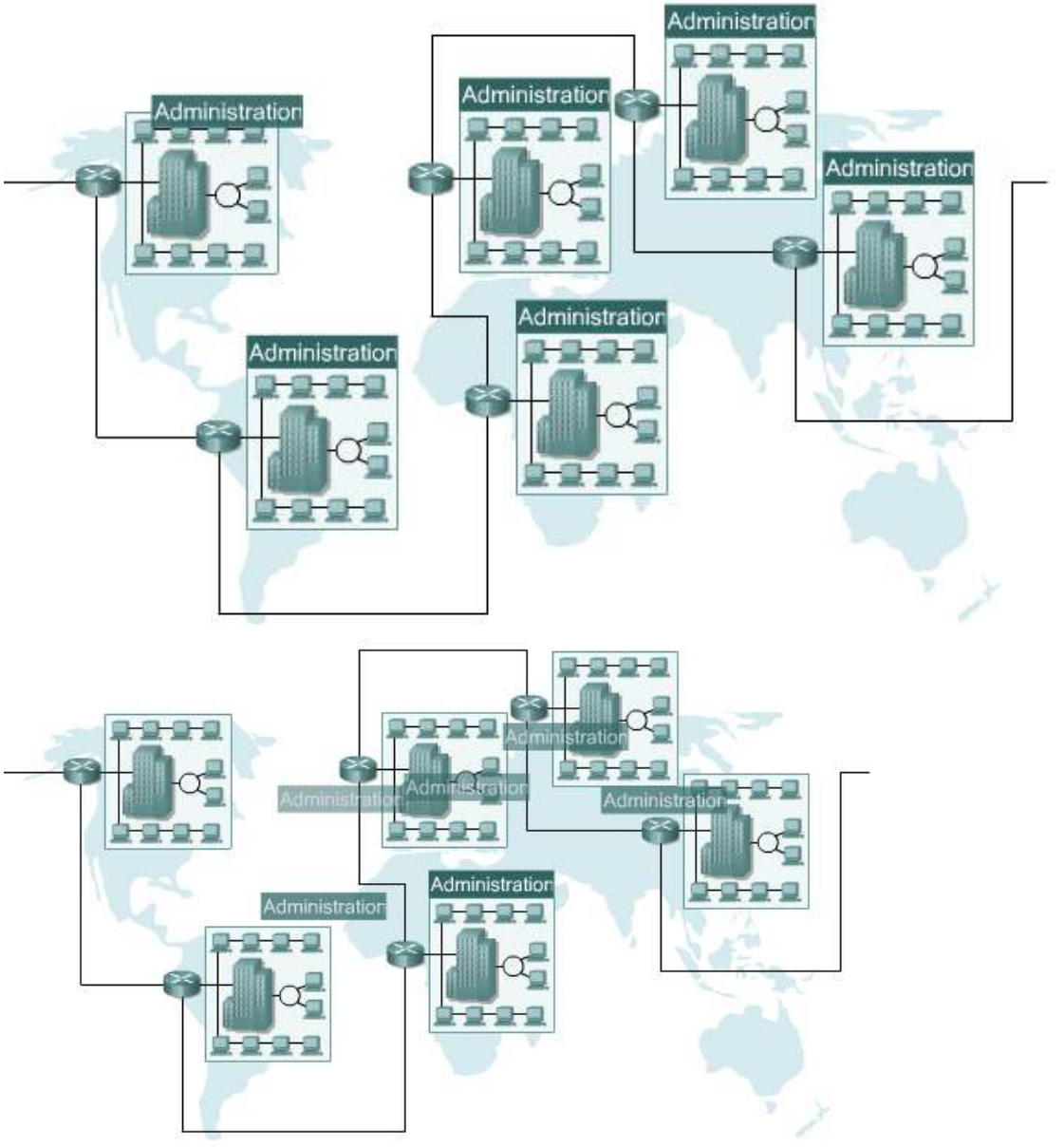

Fenêtre contextuelle
Au fur et à mesure de leur croissance, les entreprises ouvraient des agences commerciales régionales dans le monde entier. Chaque agence possédait son réseau LAN, ses logiciels, son matériel et son administrateur réseau. Chacun des services était performant, mais électroniquement isolé de tous les autres. Cette situation a souvent été une cause d'inefficacité à l'échelle de l'entreprise ; les délais d'accès aux informations à partager étaient par ailleurs rallongés.
Administration
Administration
Administration
Administration
Administration
Administration
Administration

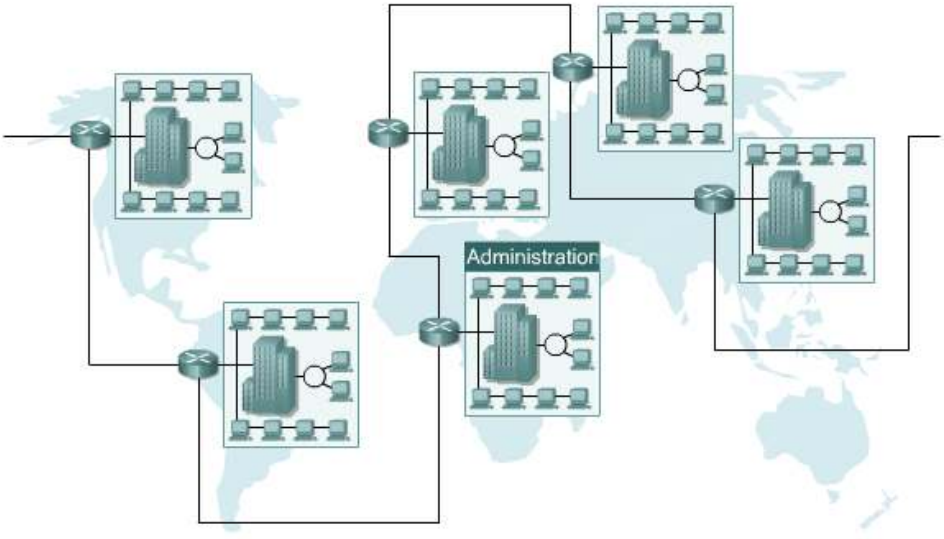
Il fallait une nouvelle technologie pour partager les informations de façon efficace et rapide au sein de l'entreprise comme entre les entreprises. 5


Administration
Administration
Administration
Administration
Administration
Administration
Administration
Fenêtre contextuelle
Trois problèmes ont engendré le besoin d'interconnecter les réseaux : les équipements et les ressources en double, l'impossibilité de communiquer avec tout le monde, dans tout lieu et à tout instant, et une administration de réseau LAN insuffisante. Pour les entreprises, ces problèmes ont été l'occasion de développer des solutions d'interconnexion à la fois pour les réseaux LAN et pour les réseaux WAN.




Administration
tration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration


Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration
Administration



La solution du moment fut de créer des réseaux métropolitains (MAN) et des réseaux étendus (WAN). Comme les réseaux WAN pouvaient relier des réseaux utilisateurs géographiquement éloignés, ils permettaient aux entreprises de communiquer entre elles sur de grandes distances. La figure

Distance entre les unités centrales	Emplacement des	Nom
0.1 m	Circuit imprimé Assistant personnel	Carte mère Réseau personnel (PAN)
1.0 m	Millimètre Mainframe	Réseau de systèmes informatiques
10 m	Pièce	Réseau local (LAN) Votre salle de cours
100 m	Bâtiment	Réseau local (LAN) Votre école
1000 m = 1 km	Campus	Réseau local (LAN) Université de Stanford
100,000 m = 100 km	Pays	Réseau WAN Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continent	Réseau WAN Afrique
10,000,000 m = 10,000 km	Planète	Wide area network (WAN) The Internet
100,000,000 m = 100,000 km	Système Terre-Lune	Réseau WAN Satellites terrestres et artificiels

illustre les tailles relatives des réseaux locaux et des réseaux étendus.

La page suivante présente l'historique des réseaux informatiques.

2.1 Terminologie de réseau

2.1.2 Historique des réseaux

Cette page présente une vue simplifiée de l'évolution d'Internet.

L'histoire des réseaux informatiques est assez complexe. 1

Chronologie Internet	
Avant 1900	Communications sur de longues distances par l'intermédiaire d'un messager, d'un cavalier, de signaux de fumée, d'un pigeon voyageur ou du télégraphe
Années 189(	Bell invente le téléphone ; le service téléphonique s'étend rapidement.
1901	Première transmission transatlantique sans fil par Marconi
Années 20	Radio AM
1939	Radio FM
Années 40	La 2e guerre mondiale favorise le développement de la radio et de la communication par micro-ondes.
1947	Shockley, Barden et Brittain inventent le transistor.
1948	Claude Shannon publie " A Theory of Electronic Communication " (Théorie de la communication électronique).
Années 50	Invention des circuits intégrés
1957	Le ministère de la Défense américain crée ARPA.
Années 60	Développement des mainframes
1962	Paul Baran de RAND travaille sur les réseaux " à commutation de paquets ".
1967	Larry Roberts publie le premier article sur ARPANET.
1969	ARPANET est établi dans les universités UCLA, UCSB, de Stanford et de l'Utah.
Années 70	Emploi généralisé des circuits intégrés numériques ; apparition des ordinateurs personnels.
1970	ALOHANET est développé par l'Université d'Hawaï.
1972	Ray Tomlinson crée un programme pour envoyer des messages électroniques.
1973	Bob Kahn et Vint Cerf commencent à travailler sur ce qui est plus tard devenu TCP/IP. ARPANET s'internationalise avec des connexions à l'University College de Londres et au Royal Radar Establishment en Norvège.
1974	BBN ouvre Telnet, la première version commerciale d'ARPANET.
Années 80	Utilisation généralisée des ordinateurs personnels et des mini-ordinateurs Unix
1981	Le terme Internet est attribué à une série de réseaux interconnectés.
1982	L'ISO publie le modèle et les protocoles OSI ; les protocoles disparaissent mais le modèle reste une référence importante.
1983	TCP/IP (Transmission Control Protocol/Internet Protocol) devient le langage universel d'Internet. ARPANET est divisé en ARPANET et MILNET.
1984	Fondation de Cisco Systems ; début du développement des routeurs et des passerelles. Introduction de DNS (Domain Name Service - service de noms

	de domaines). Le nombre d'hôtes Internet dépasse le millier.
1986	Création de NSFNET (avec une vitesse de backbone de 56 Ko/s).
1987	Le nombre d'hôtes Internet dépasse les 10 000.
1988	DARPA forme la CERT (Computer Emergency Response Team).
1989	Le nombre d'hôtes Internet dépasse les 100 000.
1990	ARPANET devient Internet.
1991	Naissance du Web (WWW). Tim Berners-Lee développe le code pour le Web.
1992	Constitution de l'ISOC (Internet Society). Le nombre d'hôtes Internet dépasse le million.
1993	Disponibilité de Mosaic, premier navigateur Web à interface graphique.
1994	Lancement de Netscape Navigator
1996	Le nombre d'hôtes Internet dépasse les 10 millions. Internet couvre toute la planète.
1997	Constitution de l'ARIN (American Registry for Internet Numbers) Mise en ligne d'Internet 2
Fin des années 90 à ce jour	Doublement du nombre des utilisateurs Internet tous les 6 mois (croissance exponentielle)
1998	Cisco réalise 70 % de ses ventes via Internet ; lancement de Networking Academies.
1999	Le réseau de backbone Internet 2 déploie IPv6. Course des grandes entreprises pour la convergence voix, vidéo et données
2001	Le nombre d'hôtes Internet dépasse les 110 millions.

Des acteurs du monde entier y ont participé ces 35 dernières années. Cette page présente une vue simplifiée de l'évolution d'Internet. Les processus d'invention et de commercialisation sont bien plus complexes, mais il est utile d'examiner le développement de fond.

Dans les années 40, les ordinateurs étaient de gigantesques machines électromécaniques sujettes à des pannes fréquentes. En 1947, l'invention du semi-conducteur ouvrit de nombreuses perspectives pour réaliser des ordinateurs plus petits et plus fiables. Dans les années 50, les grandes organisations commencèrent d'utiliser de gros ordinateurs de gestion fonctionnant avec des programmes sur cartes perforées. À la fin des années 1950 apparut le circuit intégré, qui combinait alors quelques transistors –il en comporte aujourd'hui des millions- sur une minuscule «puce» de matériau semi-conducteur. Dans les années 60, la mode était aux ordinateurs centraux desservant des terminaux et l'usage des circuits intégrés se répandit encore davantage.

À la fin des années 60 et au cours des années 70, de plus petits ordinateurs, appelés mini-ordinateurs, furent créés. Cependant, ces ordinateurs étaient encore très grands par rapport à aujourd'hui. En 1977, Apple Computer lança le premier micro-ordinateur, également appelé Mac. En 1981, IBM introduisit son premier PC. Le Mac, convivial, le PC IBM à architecture ouverte et la poursuite de la miniaturisation des circuits intégrés donnèrent naissance aux micro-ordinateurs utilisés tant à la maison qu'au bureau.

Au milieu des années 80, les utilisateurs de PC commencèrent à utiliser des modems pour partager des fichiers avec d'autres ordinateurs. C'est ce que l'on appelle encore la communication point-à-point ou par ligne téléphonique. Ce concept se développa du fait de l'utilisation d'ordinateurs comme point central de communication dans la connexion par ligne téléphonique : les BBS (*bulletin board*). Les utilisateurs pouvaient se connecter aux BBS, laisser et relever des messages et télécharger des fichiers. Ce type de système présentait l'inconvénient de ne permettre qu'une communication directe très limitée, et seulement avec les utilisateurs qui

connaissaient l'existence du BBS. L'autre limitation était que l'ordinateur BBS avait besoin d'un modem pour chaque connexion. Ainsi, si cinq personnes se connectaient simultanément, il fallait disposer de cinq modems sur cinq lignes distinctes. Ce système ne pouvait résister longtemps à l'augmentation du nombre des utilisateurs. Imaginez en effet le cas de figure où 500 personnes souhaitaient se connecter en même temps.

Entre les années 60 et 90, le ministère américain de la Défense (DoD) développa de grands réseaux étendus (WAN) fiables à des fins militaires et scientifiques. Cette technologie était différente de celle mise en œuvre pour la communication point-à-point typique des BBS. Elle permettait à plusieurs ordinateurs de s'interconnecter en empruntant différents chemins. C'est le réseau lui-même qui déterminait comment transférer les données d'un ordinateur à l'autre. Il était possible d'atteindre plusieurs ordinateurs à la fois en utilisant une seule connexion. Le réseau étendu développé par le ministère américain de la Défense devint plus tard le réseau Internet.

La page suivante traite des équipements de réseau.

2.1 Terminologie de réseau

2.1.3 Équipements de réseau

Cette page introduit les principaux équipements rencontrés sur un réseau.

On appelle équipement tout matériel qui se connecte directement à un segment du réseau. Il y a deux catégories d'équipement. La première est celle des équipements d'utilisateur final. Ces équipements sont notamment les ordinateurs, imprimantes, scanneurs et autres matériels qui fournissent des services directement à l'utilisateur. La deuxième catégorie est celle des équipements de réseau. Elle comprend tout le matériel servant à interconnecter les équipements d'utilisateur final pour leur permettre de communiquer.

Les équipements d'utilisateur final qui fournissent une connexion à un réseau sont également appelés hôtes. 1



Ces équipements permettent aux utilisateurs de partager, créer et obtenir des informations. Les équipements hôtes peuvent exister indépendamment du réseau, mais leurs capacités sont alors considérablement réduites. Les équipements hôtes sont connectés physiquement au média de réseau au moyen de cartes réseau (*NIC*). Ils utilisent cette connexion pour envoyer du courrier électronique, imprimer des rapports, numériser des images ou accéder à des bases de données. 2

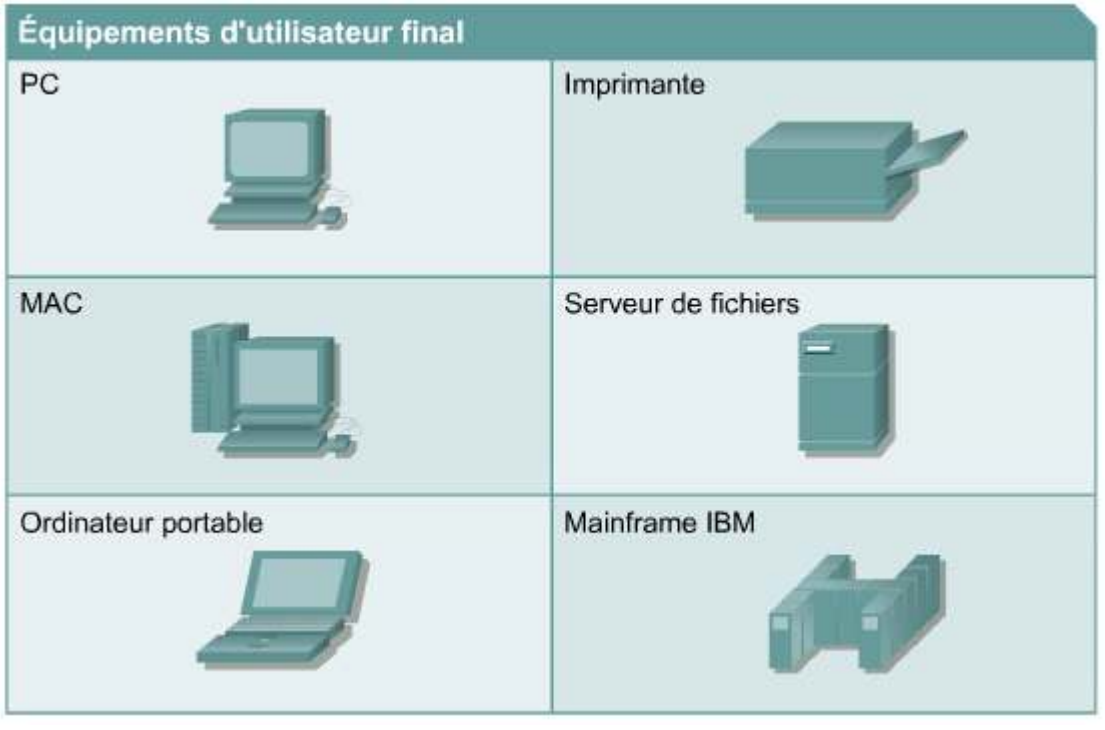


Une carte réseau est une carte de circuits imprimés qui se loge dans le connecteur d'extension d'un bus sur la carte mère d'un ordinateur. Elles existent également sous forme de périphérique. On emploie également le terme d'adaptateur réseau. Sur les ordinateurs portables, la carte réseau a généralement la taille d'une carte PCMCIA. 3



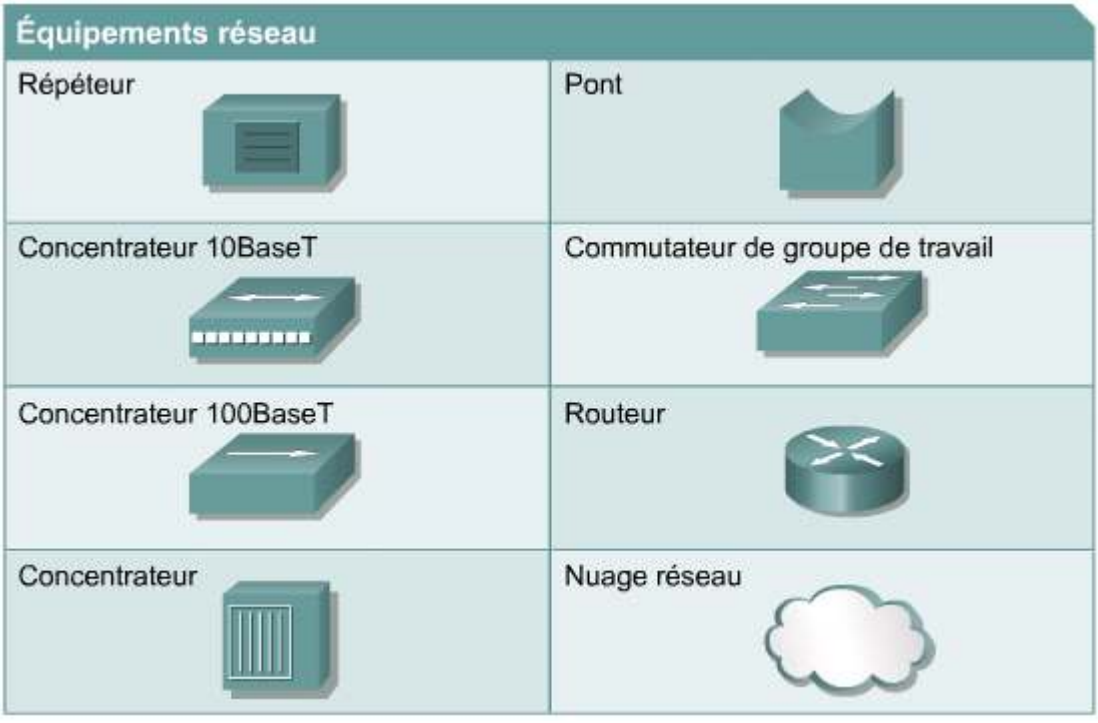
Chaque carte réseau est identifiée par un code unique appelé adresse MAC (*Media Access Control*). Cette adresse permet de contrôler la communication des données de l'hôte sur le réseau. Nous aborderons ce sujet plus en détail ultérieurement. Comme son nom l'indique, la carte réseau contrôle l'accès des hôtes au réseau.

L'industrie des réseaux n'a pas défini de symboles normalisés pour représenter les équipements d'utilisateur final. 4



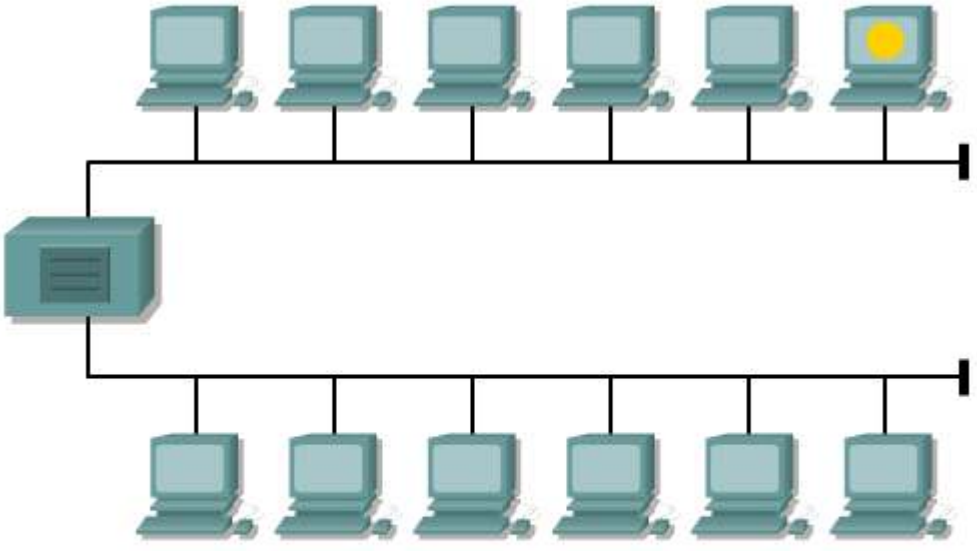
Chaque équipement est représenté fidèlement pour une reconnaissance rapide.

Les équipements de réseau assurent le transport des données qui doivent être transférées entre les équipements d'utilisateur final. 5

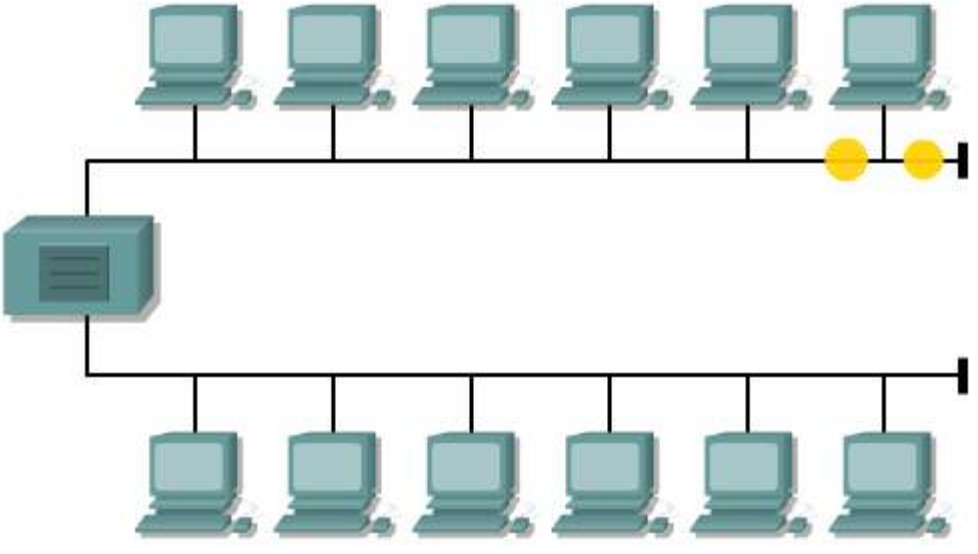


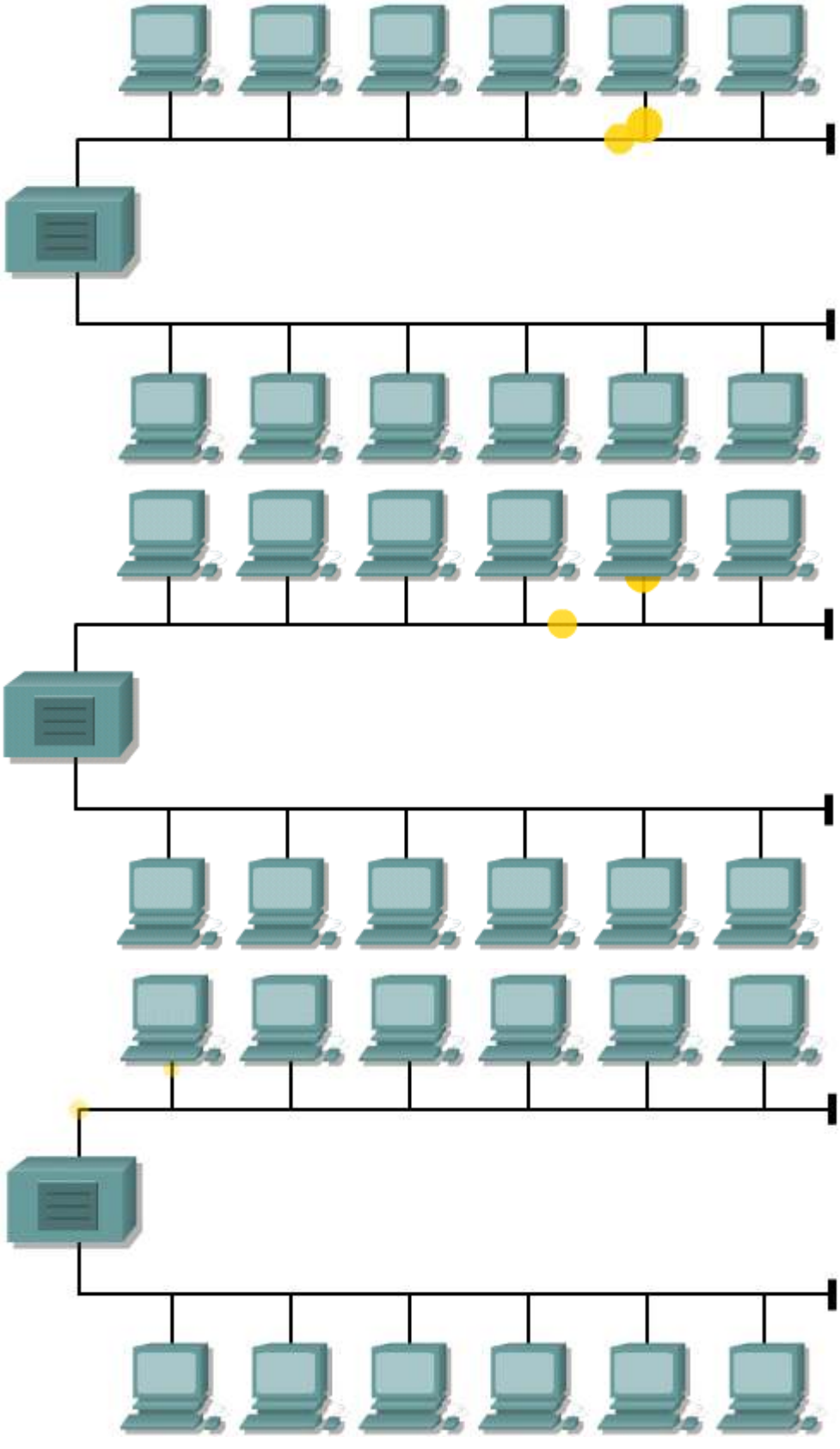
Les équipements de réseau sont utilisés pour étendre les connexions de câbles, concentrer les connexions, convertir les formats de données et gérer les transferts de données. Les répéteurs, concentrateurs, ponts, commutateurs et routeurs sont des exemples d'équipements qui assurent ces fonctions. Tous les équipements de réseau mentionnés ici sont traités de façon approfondie plus loin dans ce cours. Pour le moment, voici un bref descriptif de chacun de ces équipements.

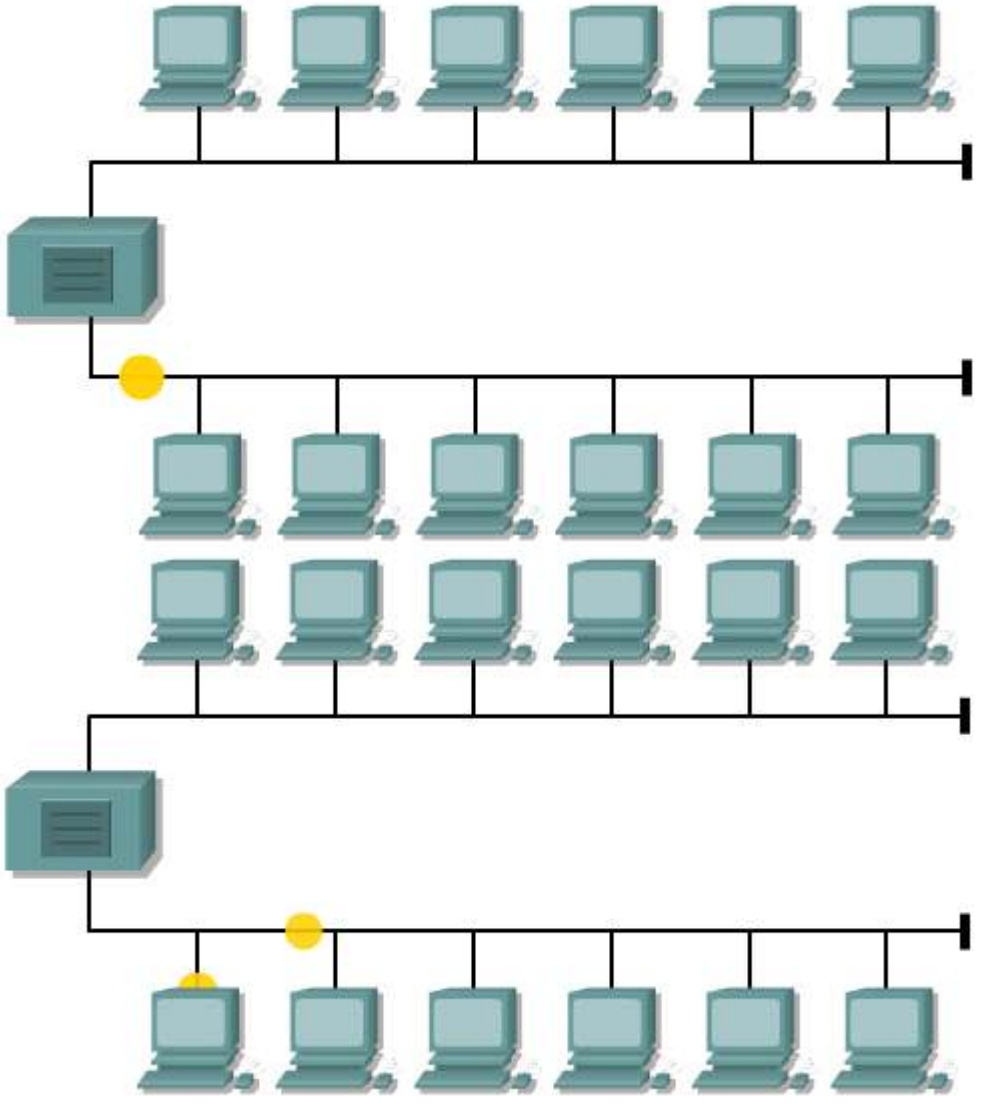
Un répéteur est un équipement réseau qui sert à régénérer un signal. Les répéteurs régénèrent les signaux analogiques ou numériques qui sont déformés par la perte de transmission due à l'atténuation. Contrairement à un routeur, un répéteur n'effectue pas un routage intelligent. 6

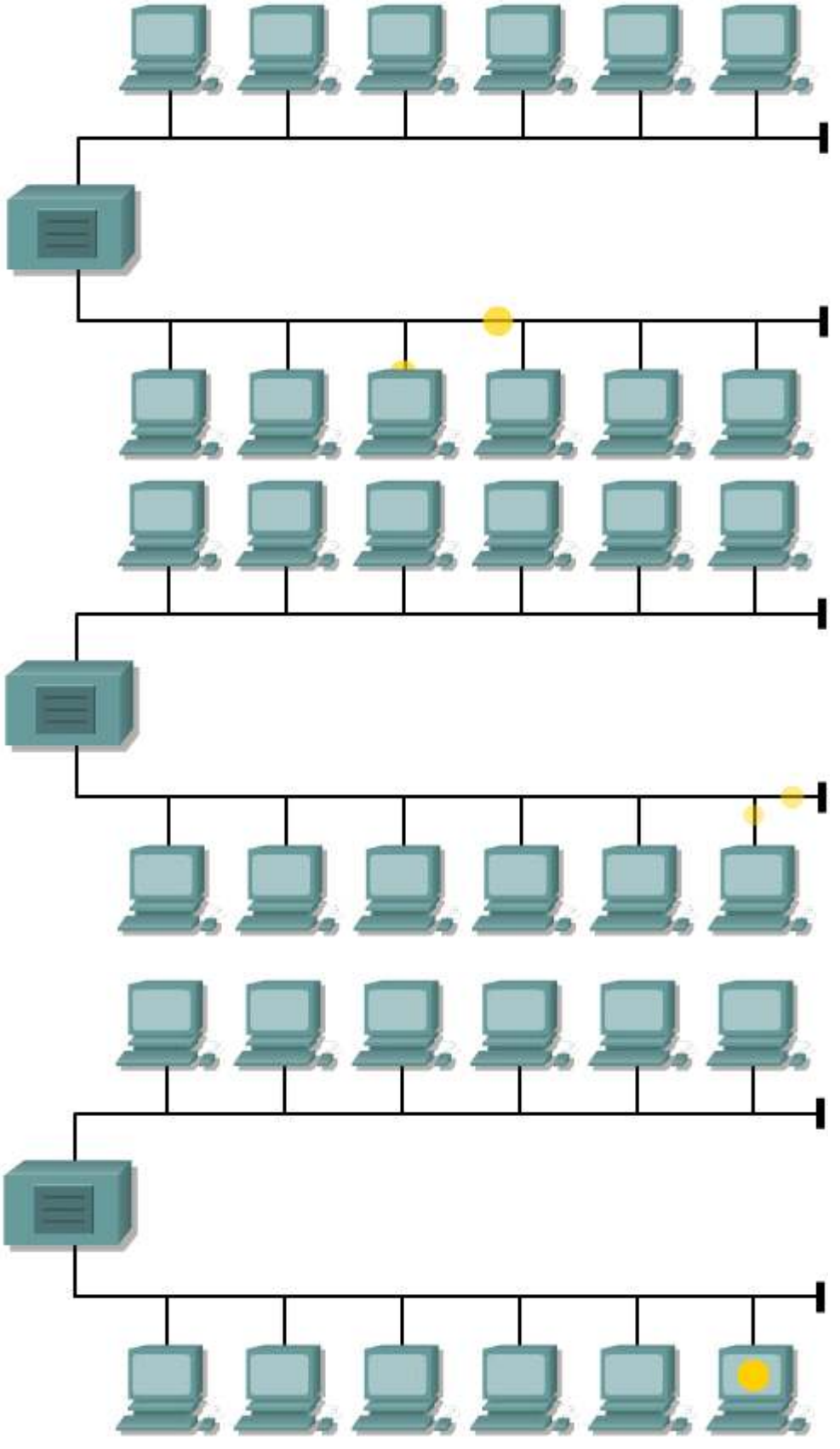


Le but du répéteur est de régénérer et de resynchroniser les signaux réseau au niveau du bit. Ils peuvent ainsi parcourir une plus longue distance dans le média.



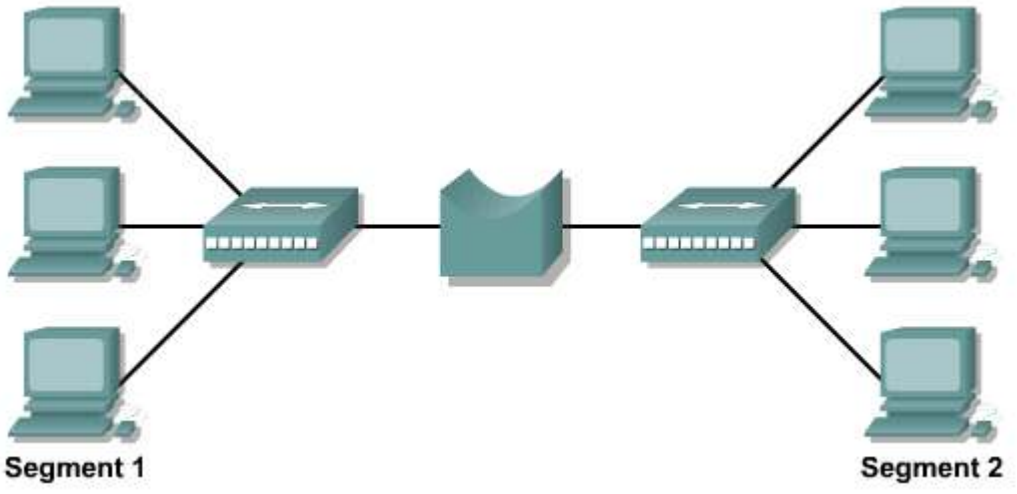






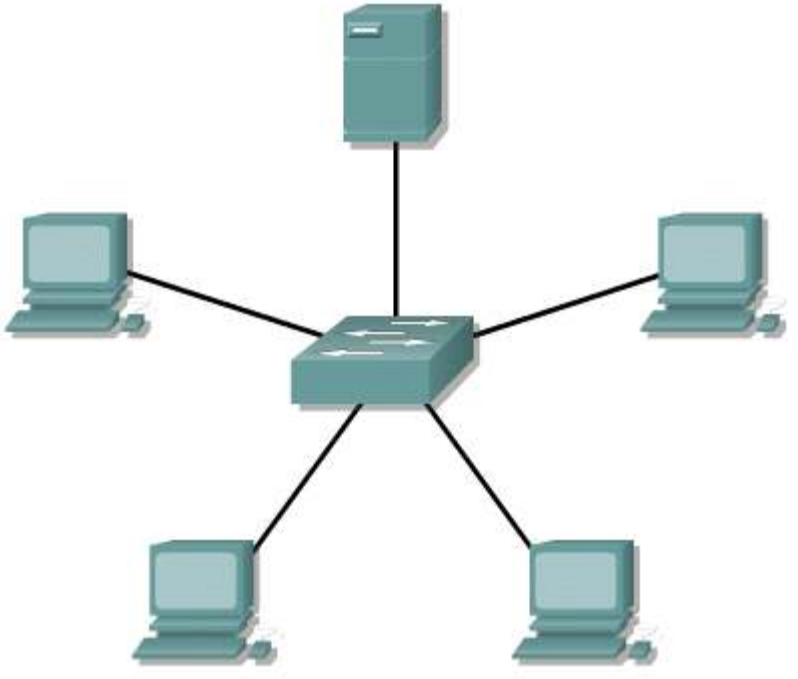
Les concentrateurs concentrent des connexions. En d'autres termes, ils rassemblent un groupe d'hôtes et permettent au réseau de les voir comme une seule unité. Cela est effectué de façon passive, sans aucun autre effet sur la transmission des données. Les concentrateurs actifs concentrent les hôtes et régénèrent également les signaux.

Les ponts convertissent les formats des données réseau et effectuent une gestion élémentaire de la transmission des données. 7



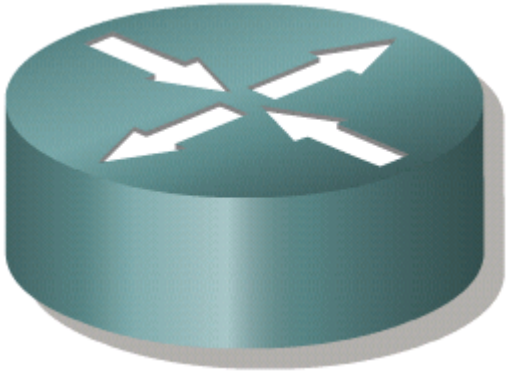
Les ponts assurent les connexions entre les différents réseaux locaux. Ils contrôlent également les données afin de déterminer si elles peuvent les traverser. Chaque partie du réseau est ainsi plus efficace.

Les commutateurs de groupe de travail apportent de l'intelligence à la gestion du transfert des données. 8



Ils sont capables de déterminer si les données doivent rester sur un réseau local et de ne les transférer que vers la connexion qui en a besoin. Une autre différence entre un pont et un commutateur réside dans le fait qu'un commutateur ne convertit pas les formats de transmission de données.

Les routeurs offrent l'ensemble des capacités précédemment citées. 9



Les routeurs peuvent régénérer les signaux, concentrer plusieurs connexions, convertir les formats de transmission de données et gérer les transferts de données. Ils peuvent également se connecter à un réseau étendu, ce qui leur permet d'interconnecter des réseaux locaux séparés par de grandes distances. Aucun des autres équipements ne peut fournir ce type de connexion.

Les activités de média interactives permettront aux étudiants de se familiariser d'avantage avec les équipements de réseau.

La page suivante introduit quelques types courants de topologies réseau.

Activité de média interactive

Glisser-Positionner: Identification des équipements de réseau

À la fin de cette activité, l'étudiant doit être en mesure d'identifier les différents équipements de réseau

Activité de média interactive

Agrandissement: Microconcentrateur Cisco 1503

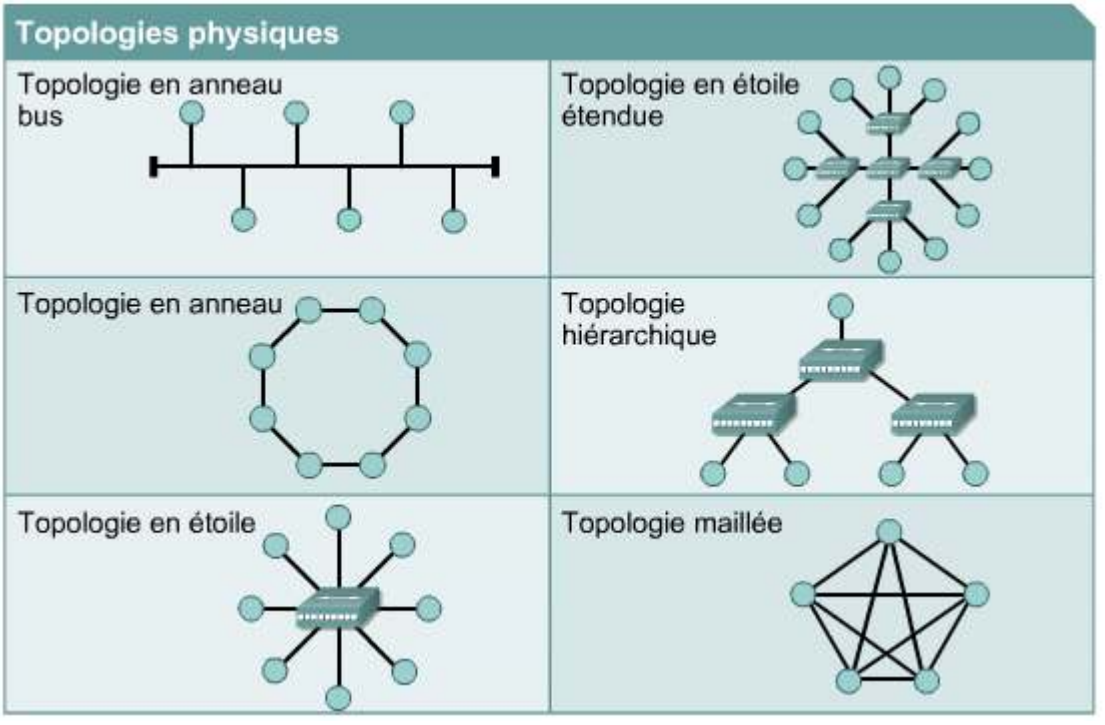
Dans cette vue agrandie, l'étudiant peut voir un concentrateur Cisco 1503.

2.1 Terminologie de réseau

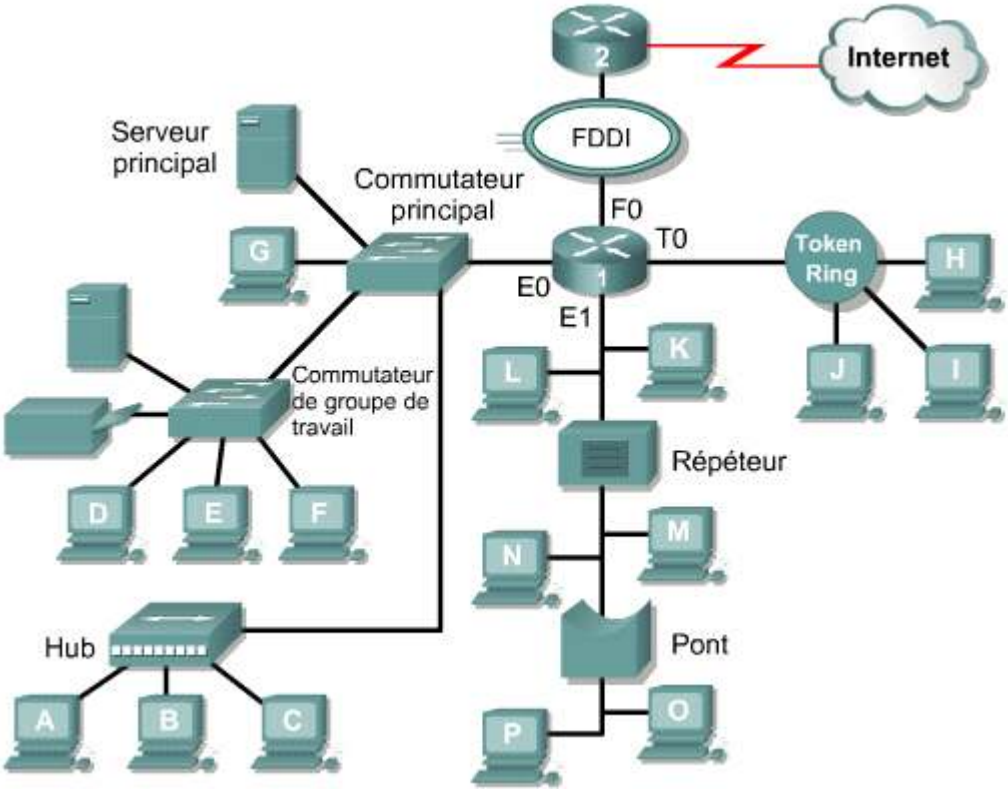
2.1.4 Topologie de réseau

Cette page présente les topologies physiques et logiques de réseau les plus courantes.

La topologie réseau définit la structure du réseau. La topologie est définie en partie par la topologie physique, qui est la configuration proprement dite du câblage ou du média. L'autre partie est la topologie logique, qui définit de quelle façon les hôtes accèdent aux médias pour envoyer des données. Les topologies physiques couramment utilisées sont les suivantes: 1



2



- Une topologie de bus fait appel à un câble de backbone unique qui est terminé aux deux extrémités. Tous les hôtes se connectent directement à ce backbone.
- Dans une topologie en anneau, chaque hôte est connecté à son voisin. Le dernier hôte se connecte au premier. Cette topologie crée un anneau physique de câble.

- Dans une topologie en étoile, tous les câbles sont raccordés à un point central.
- Une topologie en étoile étendue relie des étoiles individuelles en connectant les concentrateurs ou les commutateurs. Cette topologie peut étendre la portée et la couverture du réseau.
- Une topologie hiérarchique est similaire à une topologie en étoile étendue. Cependant, plutôt que de lier les concentrateurs ou commutateurs ensemble, le système est lié à un ordinateur qui contrôle le trafic sur la topologie.
- On implémente une topologie maillée afin de garantir une protection maximale contre l'interruption de service. Par exemple, une topologie maillée représente une solution idéale pour les systèmes de contrôle en réseau d'une centrale nucléaire. Comme vous pouvez le voir dans le schéma, chaque hôte possède ses propres connexions à tous les autres hôtes. Bien qu'Internet emprunte de multiples chemins pour atteindre un emplacement, il n'adopte pas une topologie complètement maillée.

La topologie logique d'un réseau détermine de quelle façon les hôtes communiquent sur le média. Les deux types de topologie logiques les plus courants sont le broadcast et le passage de jeton.

L'utilisation d'une topologie de broadcast indique que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau. Les stations peuvent utiliser le réseau sans suivre un ordre déterminé. Ethernet fonctionne ainsi, comme nous l'expliquerons plus loin dans le cours.

La deuxième topologie logique est le passage de jeton. Dans ce type de topologie, un jeton électronique est transmis de façon séquentielle à chaque hôte. Dès qu'un hôte reçoit le jeton, cela signifie qu'il peut transmettre des données sur le réseau. Si l'hôte n'a pas de données à transmettre, il passe le jeton à l'hôte suivant et le processus est répété. Token Ring et FDDI (*Fiber Distributed Data Interface*) sont deux exemples de réseaux qui utilisent le passage de jeton. Arcnet est une variante de Token Ring et de FDDI. Il s'agit d'un passage de jeton sur une topologie de bus.

Le schéma de la figure 2 illustre de nombreuses topologies différentes raccordées par des équipements de réseau. Il représente un réseau de complexité moyenne, comme celui qu'on retrouve habituellement dans une école ou une petite entreprise. Le schéma comporte de nombreux symboles et concepts de réseau dont l'apprentissage peut prendre du temps.

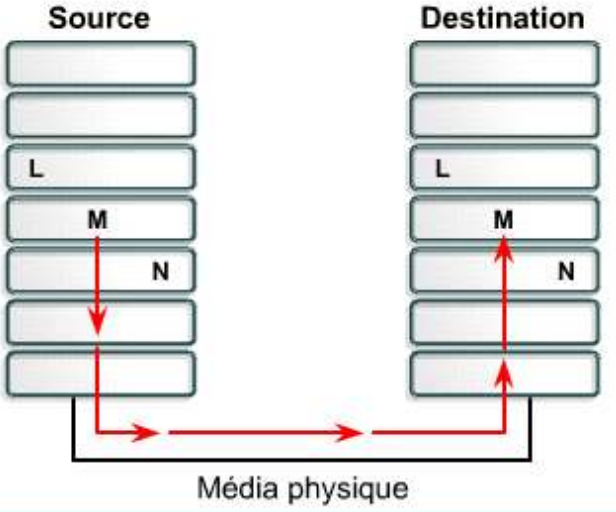
La page suivante traite des protocoles de réseau.

2.1 Terminologie de réseau

2.1.5 Protocoles de réseau

Cette page décrit les protocoles réseau et explique leur importance.

Les suites de protocoles sont des ensembles de protocoles qui permettent à des hôtes de communiquer sur un réseau. Un protocole est une description formelle d'un ensemble de règles et de conventions qui régissent un aspect particulier de la façon dont les équipements communiquent sur un réseau. Les protocoles déterminent le format, la chronologie, le séquençage et le contrôle d'erreur dans la communication de données. Sans protocole, l'ordinateur ne peut pas constituer ou reconstruire dans le format original le flux de bits entrants provenant d'un autre ordinateur. 1



L, M, N	Couches dans notre modèle de communication entre ordinateurs
source M, destination M	Couches homologues
→	Communications entre couches homologues
Protocole de couche M	Les règles selon lesquelles la source M communique avec la destination M

Les protocoles contrôlent tous les aspects de la communication de données, dont:

- Comment est construit le réseau physique
- Comment les ordinateurs se connectent au réseau
- Comment les données sont formatées pour la transmission
- Comment ces données sont envoyées
- Comment traiter les erreurs

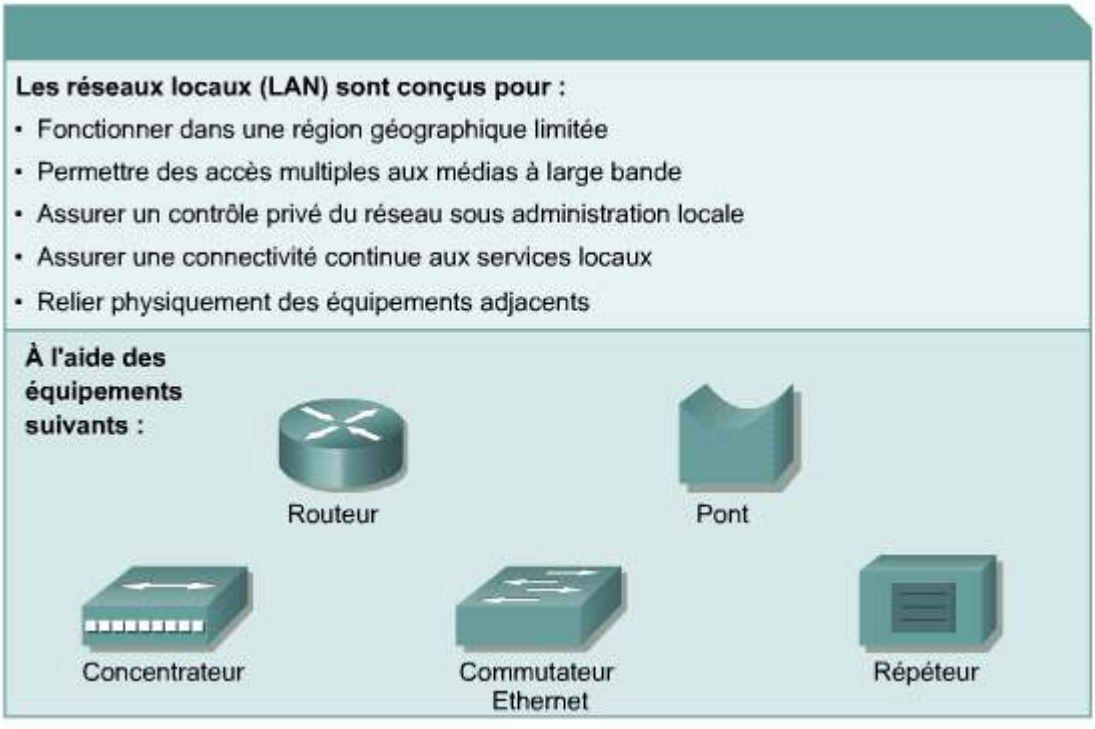
Ces règles de réseau sont créées et actualisées par un grand nombre d'organisations et de comités. Il s'agit notamment de l'IEEE (*Institute of Electrical and Electronic Engineers*), de l'ANSI (*American National Standards Institute*), de la TIA (*Telecommunications Industry Association*), de l'EIA (*Electronic Industries Alliance*), ainsi que l'ITU (*International Telecommunications Union*) précédemment nommée CCITT (*Comité Consultatif International Téléphonique et Télégraphique*).

La page suivante introduit les réseaux locaux (LAN).

2.1 Terminologie de réseau

2.1.6 Réseaux locaux (LAN)

Cette page explique les caractéristiques et les avantages des réseaux locaux. 1


Les réseaux locaux (LAN) sont conçus pour :
• Fonctionner dans une région géographique limitée
• Permettre des accès multiples aux médias à large bande
• Assurer un contrôle privé du réseau sous administration locale
• Assurer une connectivité continue aux services locaux
• Relier physiquement des équipements adjacents
À l'aide des équipements suivants :
Routeur
Pont
Concentrateur
Commutateur Ethernet
Répéteur

Les réseaux locaux comprennent les éléments suivants:

- Ordinateurs
- Cartes réseau
- Équipements périphériques
- Médias réseau
- Équipements de réseau

Les réseaux locaux permettent aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes. Le courrier électronique est un bon exemple de cette technologie. Les réseaux locaux gèrent les données, les communications locales et l'équipement informatique.

Voici quelques technologies courantes de réseau local:

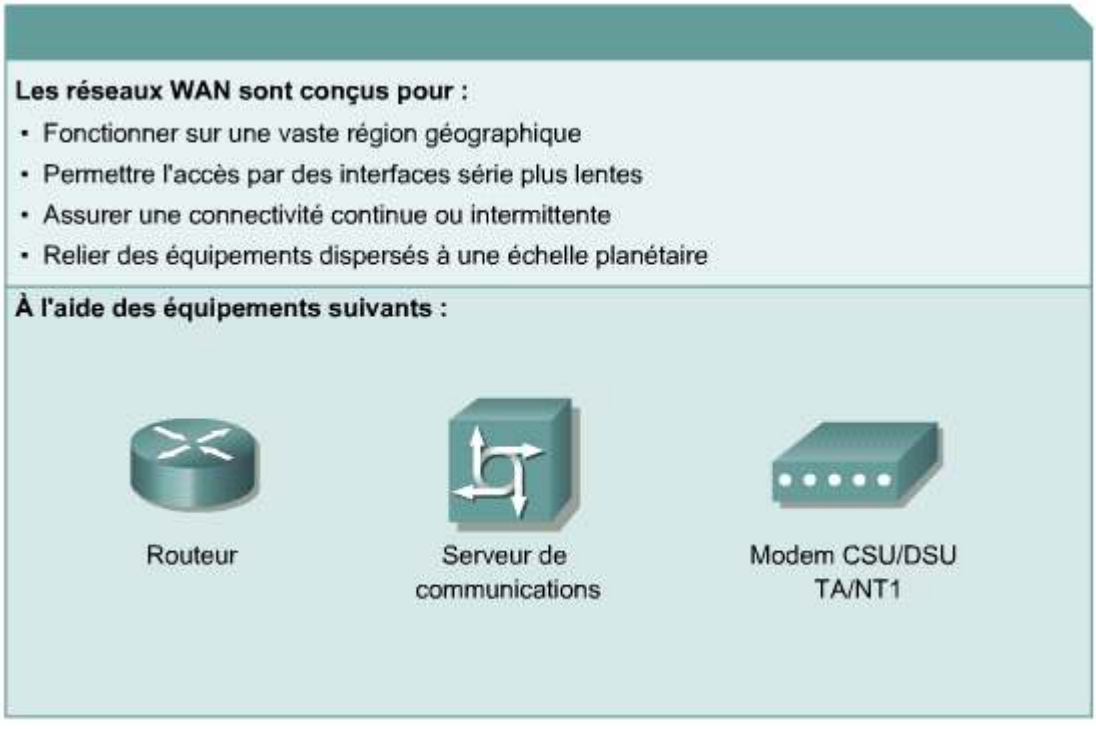
- Ethernet
- Token Ring
- FDDI

La page suivante introduira les réseaux étendus (WAN).

2.1 Terminologie de réseau

2.1.7 Réseaux étendus (WAN)

Cette page explique les fonctions d'un réseau étendu. 1


Les réseaux WAN sont conçus pour :
• Fonctionner sur une vaste région géographique
• Permettre l'accès par des interfaces série plus lentes
• Assurer une connectivité continue ou intermittente
• Relier des équipements dispersés à une échelle planétaire
À l'aide des équipements suivants :
Routeur
Serveur de communications
Modem CSU/DSU TA/NT1

Les réseaux étendus interconnectent des réseaux locaux, qui, à leur tour, donnent accès aux ordinateurs ou aux serveurs de fichiers situés en d'autres lieux. Comme les réseaux étendus relient des réseaux utilisateurs géographiquement dispersés, ils permettent aux entreprises de communiquer entre elles sur de grandes distances. Les réseaux étendus permettent le partage d'ordinateurs, imprimantes et autres équipements raccordés à un LAN situé sur un lieu distant. Les réseaux étendus fournissent des communications instantanées à l'intérieur de grandes zones géographiques.

Les logiciels de collaboration fournissent l'accès à des informations et des ressources en temps réel et permettent de tenir des réunions à distance. Les réseaux étendus ont contribué à créer une nouvelle catégorie de travailleurs appelés télétravailleurs. Ces personnes ont la possibilité de travailler sans quitter leur domicile.

Les réseaux WAN sont conçus pour effectuer les tâches suivantes:

- Fonctionner dans des zones étendues ou géographiquement dispersées
- Permettre aux utilisateurs de disposer de capacités de communication en temps réel avec d'autres utilisateurs
- Fournir des ressources distantes en temps réel connectées aux services locaux
- Fournir des services de courrier électronique, Internet, de transfert de fichiers et de commerce électronique

Voici quelques technologies courantes liées aux réseaux étendus:

- Modems
- RNIS (*Réseau Numérique à Intégration de Services*)

- DSL (*Digital Subscriber Line*)
- Frame Relay
- T1, E1, T3 et E3
- SONET (*Synchronous Optical Network*)

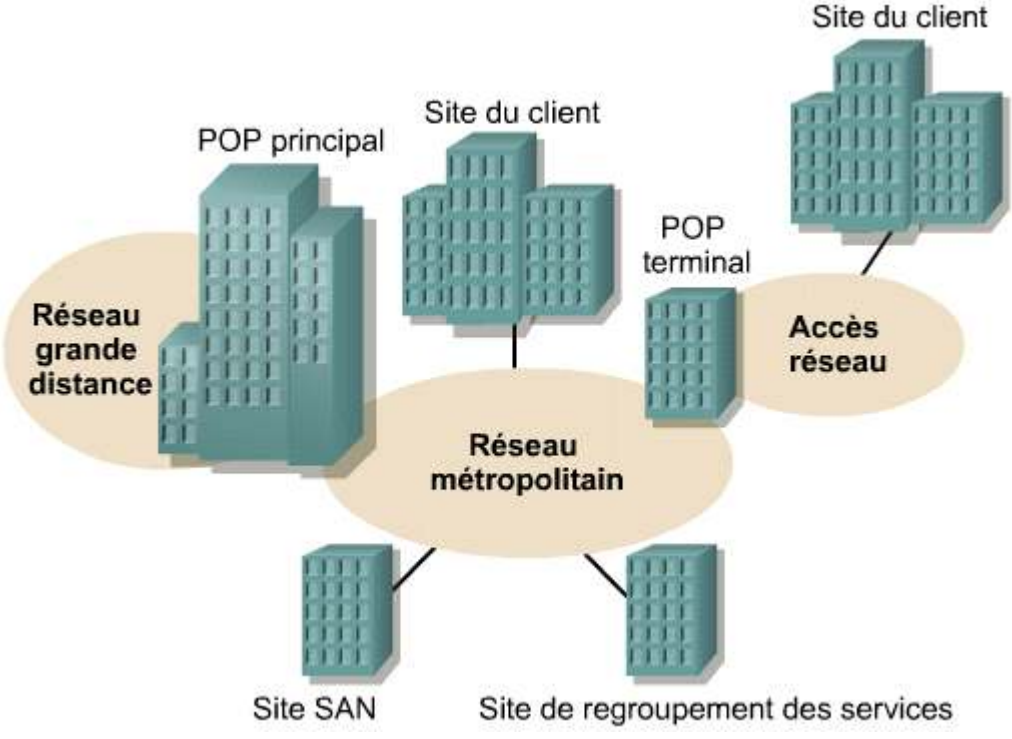
La page suivante introduira les réseaux métropolitains (MAN).

2.1 Terminologie de réseau

2.1.8 Réseaux métropolitains (MAN)

Cette page explique comment les réseaux MAN sont utilisés.

Un réseau MAN est un réseau qui s'étend à une zone métropolitaine telle qu'une ville ou une zone de banlieue. Un réseau MAN comprend habituellement au moins deux réseaux LAN situés dans une zone géographique commune. Par exemple, une banque possédant plusieurs agences peut utiliser ce type de réseau. 1



En général, on fait appel à un fournisseur de services pour connecter au moins deux sites de réseau local au moyen de lignes de communication privées ou de services optiques. Les technologies de pont sans fil qui envoient des signaux à l'intérieur de zones publiques peuvent également être utilisées pour créer un réseau MAN.

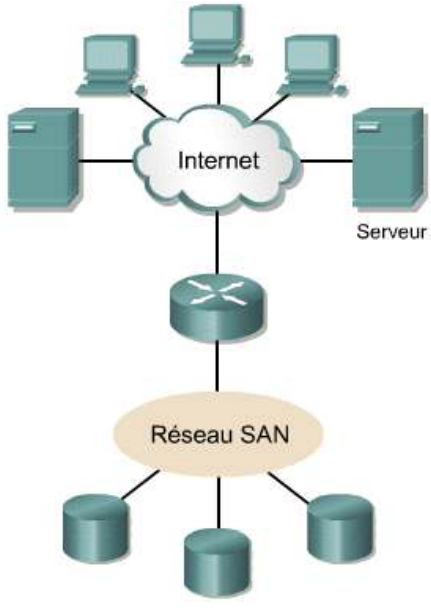
La page suivante introduira les réseaux SAN.

2.1 Terminologie de réseau

2.1.9 Réseaux SAN

Cette page décrit les caractéristiques des réseaux SAN.

Un réseau de stockage (SAN) est un réseau à haute performance dédié qui permet de transférer des données entre des serveurs et des ressources de stockage. Du fait qu'il s'agit d'un réseau dédié distinct, il évite tout conflit de trafic entre les clients et les serveurs. 1



La technologie SAN permet de bénéficier d'une connectivité haut débit pour différentes configurations : serveur/stockage, stockage/stockage ou serveur/serveur. Cette méthode recourt à une infrastructure de réseau séparée qui résout tout problème associé à la connectivité réseau existante.

Les réseaux SAN offrent les caractéristiques suivantes:

- **Performance** – les réseaux SAN permettent un accès simultané à haut débit, par deux serveurs ou plus, aux matrices de disques et de bandes. Cela améliore les performances du système.
- **Disponibilité** – Les réseaux SAN intègrent la tolérance aux sinistres. Les données peuvent être dupliquées sur un réseau SAN situé jusqu'à 10 km de distance.
- **Évolutivité** – Un réseau SAN peut utiliser les technologies les plus variées. Cela facilite le déplacement des données de sauvegarde, des opérations, la migration des fichiers et la réplication des données entre les systèmes.

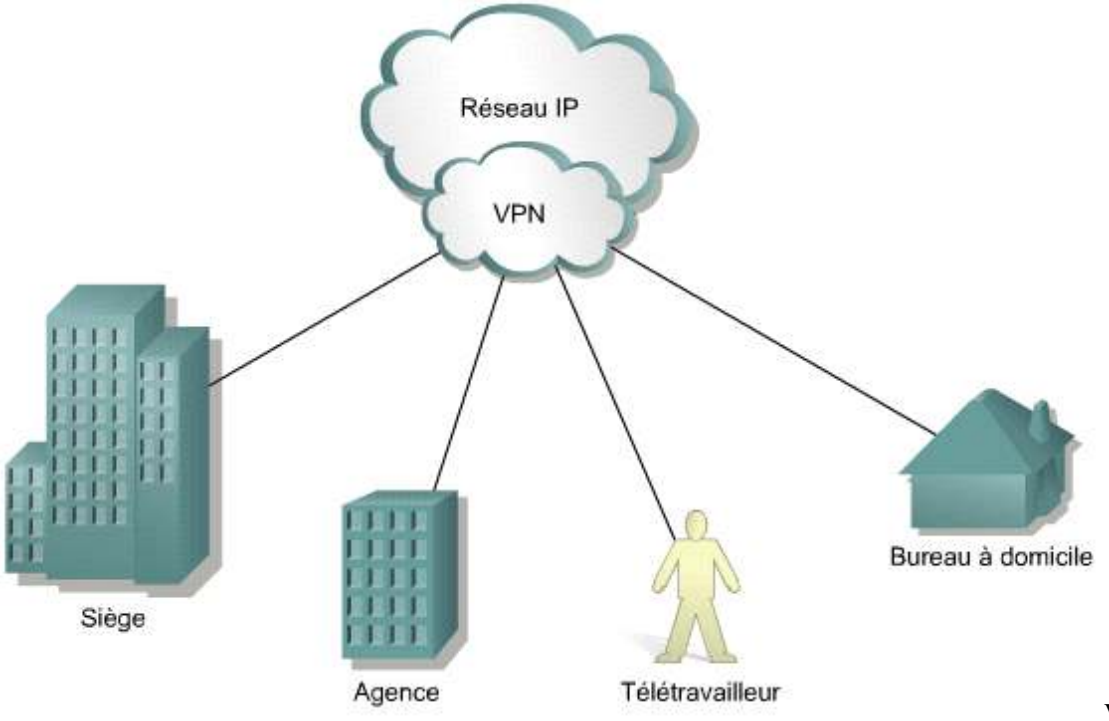
La page suivante présente les réseaux privés virtuels (VPN).

2.1 Terminologie de réseau

2.1.10 Réseau privé virtuel (VPN)

Cette page définit un VPN et décrit son utilisation.

Un réseau privé virtuel (VPN) est un réseau privé construit au sein d'une infrastructure de réseau publique telle que le réseau mondial Internet. Au moyen d'un réseau privé virtuel, un télétravailleur peut accéder à distance au réseau du quartier général de sa société. 1



Via Internet, il est possible de construire un tunnel sécurisé entre le PC du télétravailleur et un routeur VPN installé au quartier général de la société.

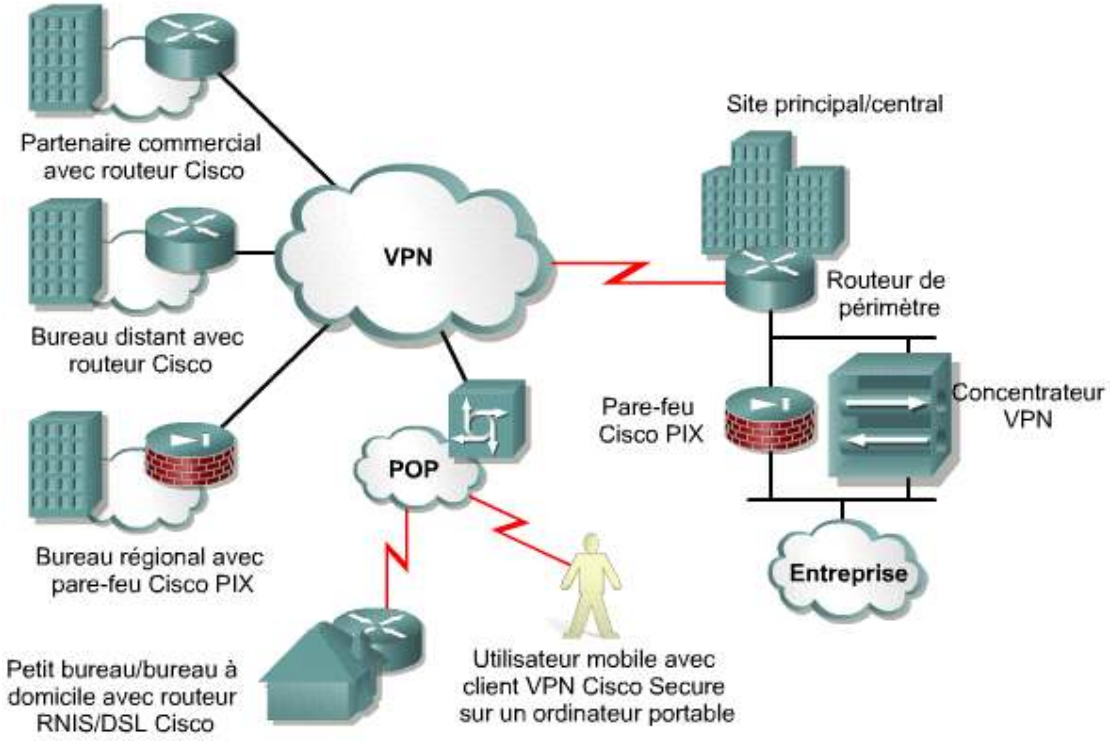
La page suivante explique les avantages des réseaux privés virtuels.

2.1 Terminologie de réseau

2.1.11 Avantages des réseaux privés virtuels

Cette page présente les trois principaux types de réseaux privés virtuels et explique leur fonctionnement.

Les produits Cisco prennent en charge les dernières technologies VPN. Un réseau privé virtuel est un service qui offre une connectivité sécurisée et fiable sur une infrastructure de réseau public partagée telle qu'Internet.
1


Partenaire commercial avec routeur Cisco
Bureau distant avec routeur Cisco
Bureau régional avec pare-feu Cisco PIX
Petit bureau/bureau à domicile avec routeur RNIS/DSL Cisco
VPN
POP
Site principal/central
Routeur de périmètre
Pare-feu Cisco PIX
Concentrateur VPN
Entreprise
Utilisateur mobile avec client VPN Cisco Secure sur un ordinateur portable

Les VPN maintiennent les mêmes politiques de sécurité et de gestion qu'un réseau privé. L'utilisation d'un réseau privé virtuel est la façon la plus rentable d'établir une connexion point-à-point entre des utilisateurs distants et un réseau d'entreprise.

Voici une liste des trois principaux types de VPN :

- Les VPN d'accès fournissent aux utilisateurs mobiles et de petits bureaux/bureaux à domicile (SOHO) l'accès distant à un intranet ou à un extranet sur une infrastructure partagée. Les VPN d'accès utilisent des technologies analogiques, d'accès par ligne téléphonique, RNIS, DSL, IP mobile et câble afin de connecter en toute sécurité les utilisateurs mobiles, les télétravailleurs et les agences.
- Les VPN d'intranet font appel à des connexions dédiées pour raccorder des bureaux régionaux et des bureaux distants à un réseau interne sur une infrastructure partagée. Les VPN d'intranet diffèrent des VPN d'extranet en ce qu'ils n'autorisent l'accès qu'aux employés de l'entreprise.
- Les VPN d'extranet utilisent des connexions dédiées pour relier des partenaires commerciaux à un réseau interne sur une infrastructure partagée. Les VPN d'extranet diffèrent des VPN d'intranet en ce qu'ils permettent l'accès aux utilisateurs en dehors de l'entreprise.

La page suivante présente les intranets et les extranets.

2.1 Terminologie de réseau

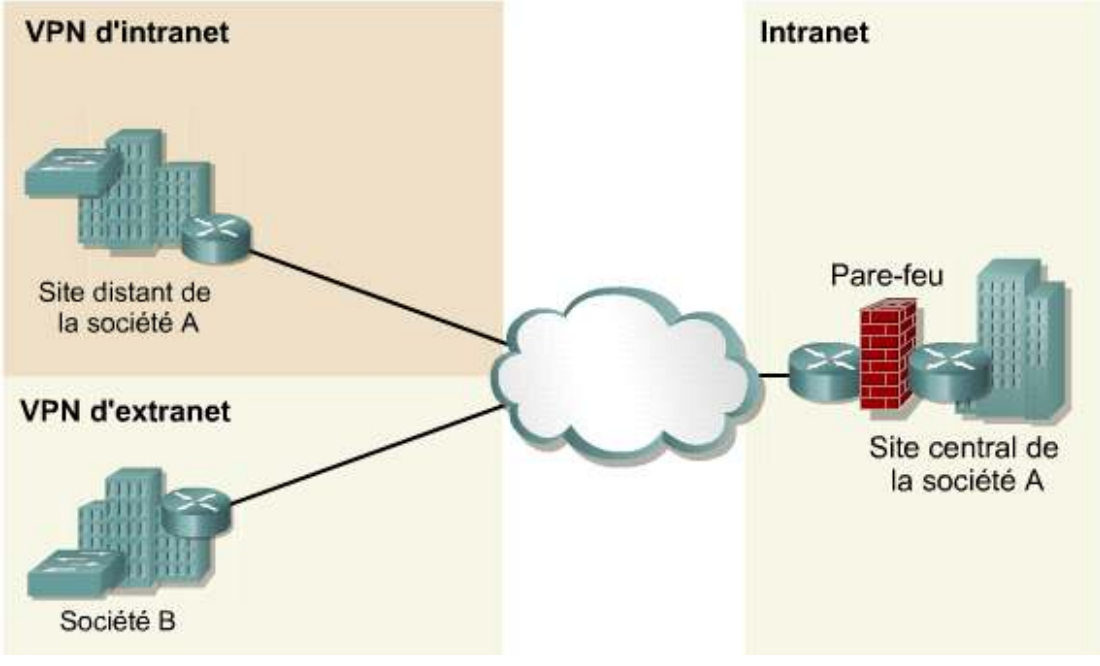
2.1.12 Intranets et extranets

Cette page présente aux étudiants les intranets et les extranets.

Un intranet est une configuration de réseau local très répandue. Les serveurs Web intranet diffèrent des serveurs Web publics en ce que le public doit posséder les autorisations et mots de passe appropriés pour accéder à l'intranet d'une organisation. Les intranets sont conçus pour autoriser les utilisateurs qui ont des privilèges d'accès à accéder au réseau local interne de l'organisation. Au sein d'un intranet, les serveurs Web sont

installés dans le réseau. La technologie de navigateur sert de frontal commun pour accéder aux informations, telles que les données financières, graphiques ou textuelles.

Le terme extranet fait référence à des applications et à des services qui sont basés sur intranet, et qui utilisent un accès étendu et sécurisé pour les utilisateurs ou entreprises externes. Cet accès s'effectue habituellement au travers de mots de passe, ID utilisateur et autres dispositifs de sécurité au niveau applicatif. Un extranet est une extension de deux stratégies intranet au moins, avec une interaction sécurisée entre les entreprises participantes et leurs intranets respectifs. 1



Cette leçon est terminée. La leçon suivante traite de la bande passante. La première page explique pourquoi la bande passante est importante.

2.2 Bande passante

2.2.1 Importance de la bande passante

Cette page décrit les quatre caractéristiques les plus importantes de la bande passante.

La bande passante est définie comme la quantité d'informations qui peut transiter sur une connexion réseau en un temps donné. Il est important de comprendre le concept de bande passante pour les raisons suivantes. 1

Pourquoi la bande passante est importante :
- La bande passante est limitée par des facteurs physiques et technologiques
- La bande passante n'est pas gratuite
- Les besoins en bande passante augmentent rapidement
- La bande passante est critique pour les performances du réseau

La bande passante est finie.Quel que soit le média qui est utilisé pour construire un réseau, il y a des limites à la capacité du réseau à transporter des informations. La bande passante est limitée par les lois de la physique et

aussi par les technologies utilisées pour placer des informations sur le média. Par exemple, la bande passante d'un modem conventionnel est limitée à environ 56 kbits/s, à la fois par les propriétés physiques des fils téléphoniques à paires torsadées et par la technologie du modem. La technologie DSL utilise les mêmes fils téléphoniques à paires torsadées. Cependant, elle délivre bien plus de bande passante que les modems conventionnels. Ainsi, même les limites imposées par les lois de la physique sont quelques fois difficiles à définir. La fibre optique possède le potentiel physique pour fournir une bande passante pratiquement illimitée. Malgré cela, la bande passante de la fibre optique ne pourra être pleinement exploitée avant que des technologies ne soient développées pour tirer pleinement parti de son potentiel.

La bande passante n'est pas gratuite.Il est possible d'acquérir des équipements pour un réseau local qui fourniront une bande passante quasiment illimitée sur une longue période. Pour les connexions WAN, il est généralement nécessaire d'acquérir de la bande passante auprès d'un fournisseur de services. Dans un cas comme dans l'autre, l'utilisateur individuel ou l'entreprise pourra faire des économies significatives en comprenant bien la notion de bande passante et l'évolution de la demande avec le temps. L'administrateur doit prendre les bonnes décisions sur les types d'équipement et de services à acheter.

La bande passante est un facteur important qui est indispensable pour analyser les performances du réseau, concevoir de nouveaux réseaux et comprendre Internet.Un professionnel des réseaux doit comprendre l'impact considérable de la bande passante et du débit sur la performance et la conception du réseau. Les informations circulent sous forme de chaîne de bits d'un ordinateur à l'autre à travers le monde. Ces bits constituent des quantités énormes d'informations qui transitent d'un bout à l'autre de la planète en quelques secondes à peine.

La demande en bande passante ne cesse de croître. Dès que des nouvelles technologies et infrastructures de réseau sont créées pour fournir une bande passante plus large, on voit apparaître de nouvelles applications qui tirent parti de cette capacité supérieure. La remise sur un réseau de contenus multimédias tels que la vidéo et l'audio en continu nécessite une quantité considérable de bande passante. Les systèmes de téléphonie IP sont à présent installés couramment à la place de systèmes vocaux traditionnels, ce qui augmente encore le besoin en bande passante. Tout professionnel de réseau digne de ce nom doit anticiper le besoin en bande passante accrue et agir en conséquence.

La page suivante expose certaines analogies qui aideront à mieux appréhender la bande passante.

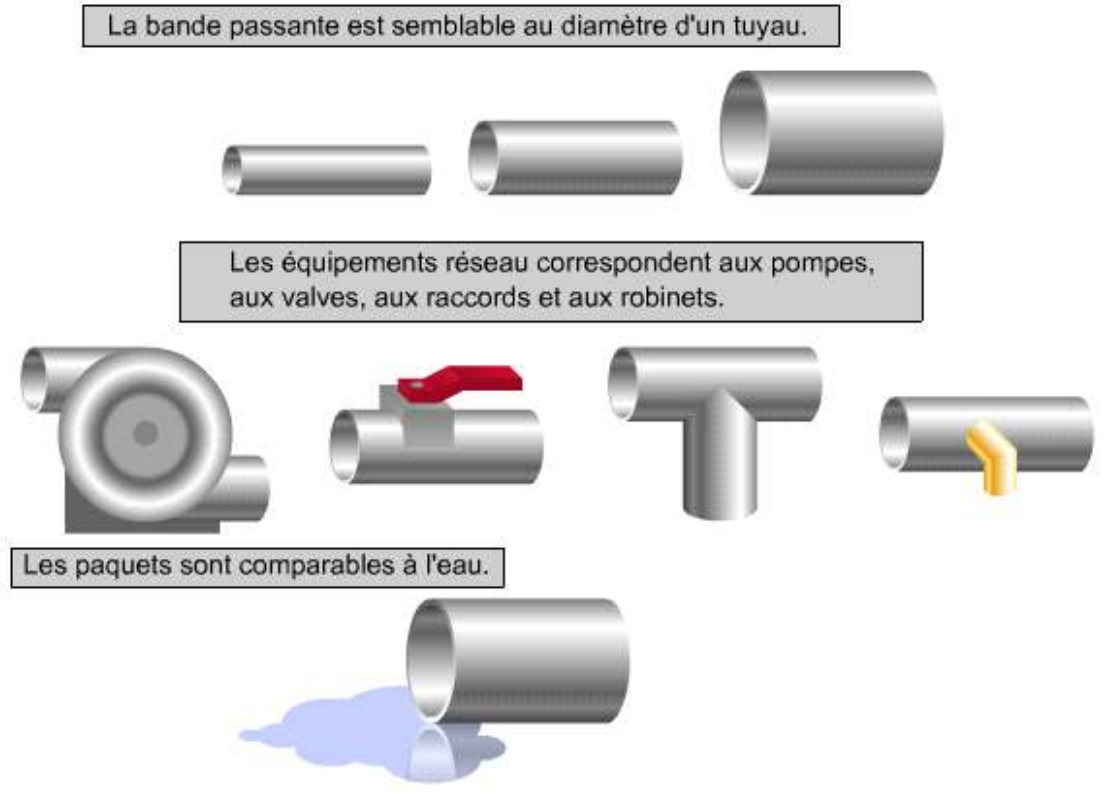
2.2 Bande passante

2.2.2 Le bureau

Cette page présente deux analogies qui peuvent vous permettre de mieux visualiser la bande passante dans un réseau.

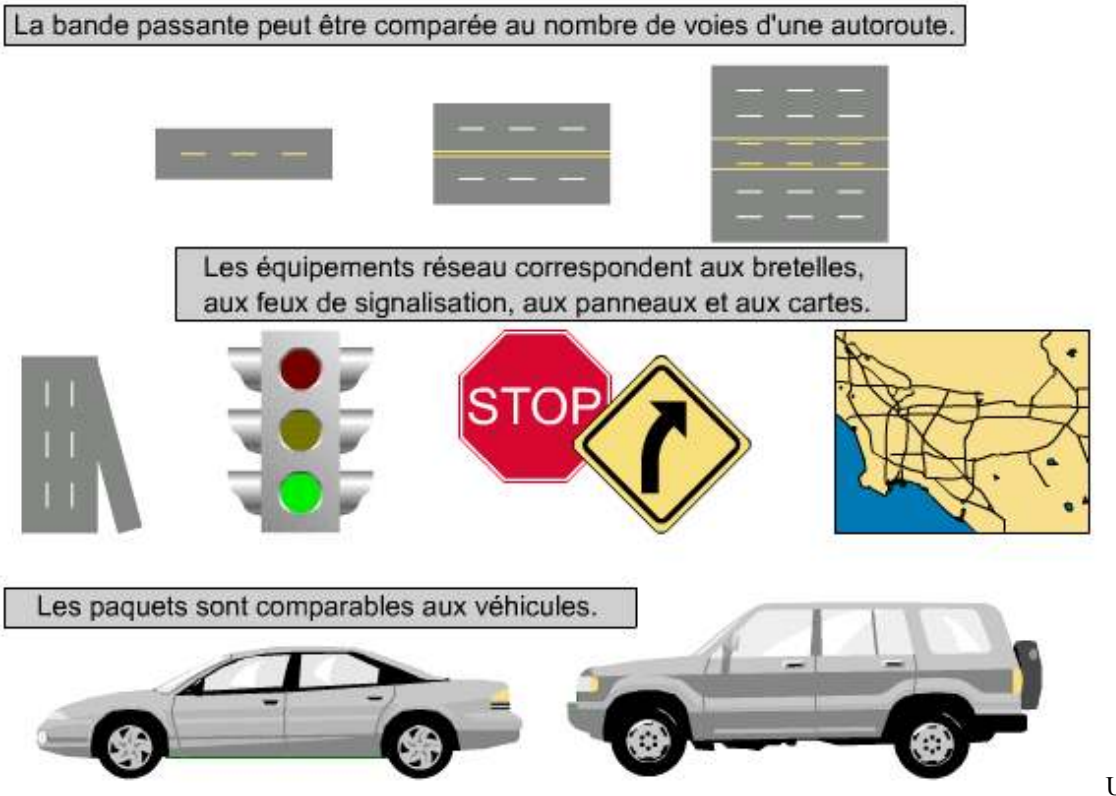
La bande passante a été définie comme la quantité d'informations qui peut transiter sur un réseau en un temps donné. Cette page présente deux analogies qui peuvent vous permettre de mieux visualiser la bande passante dans un réseau.

La bande passante est semblable au diamètre d'un tuyau. 1


La bande passante est semblable au diamètre d'un tuyau.
Les équipements réseau correspondent aux pompes, aux valves, aux raccords et aux robinets.
Les paquets sont comparables à l'eau.

Un réseau de canalisations apporte de l'eau potable à des foyers et à des entreprises et évacue les eaux usées. Ce réseau d'eau est constitué de tuyaux de différents diamètres. Le diamètre des principales canalisations d'une ville peut atteindre 2 mètres, tandis que 2 cm suffisent pour le tuyau d'un robinet de cuisine. La largeur du tuyau détermine sa capacité de transport en eau. Par conséquent, l'eau peut être comparée aux données, et la largeur du tuyau à la bande passante. Les experts réseau vous diront qu'il faut installer de plus gros tuyaux pour disposer d'une capacité de transport des informations supérieure.

La bande passante peut être comparée au nombre de voies d'une autoroute. 2


La bande passante peut être comparée au nombre de voies d'une autoroute.
Les équipements réseau correspondent aux bretelles, aux feux de signalisation, aux panneaux et aux cartes.
STOP
Les paquets sont comparables aux véhicules.

Un réseau de routes dessert chaque ville ou village. Les grandes autoroutes aux nombreuses voies sont rejointes par de plus petites routes comportant moins de voies. À leur tour, ces routes conduisent à des routes plus étroites qui mènent aux voies d'accès des résidences et des entreprises. Lorsque le système autoroutier est peu fréquenté, chaque véhicule est en mesure de se déplacer librement. Lorsqu'il y a davantage de trafic au contraire, chaque véhicule se déplace plus lentement. C'est sur les routes qui comportent le moins de voies que cela est le plus évident. Dès qu'il y a affluence sur le système routier, il y a des ralentissements, voire des bouchons, y compris sur les routes qui comportent beaucoup de voies. Un réseau de données est très semblable à un système routier. Les paquets de données sont comparables aux automobiles et la bande passante au nombre de voies de la route. En se figurant un réseau de données comme un système routier, il est facile de réaliser comment les connexions à faible bande passante peuvent provoquer la congestion du trafic dans tout le réseau.

La page suivante décrit la façon de mesurer la bande passante.

2.2 Bande passante

2.2.3 Mesures

Cette page explique comment mesurer la bande passante.

Dans les systèmes numériques, l'unité de base de la bande passante est le bit par seconde (bit/s). La bande passante est la mesure de la quantité de bits d'informations pouvant transiter d'un endroit à un autre en un temps donné. Bien que l'on puisse exprimer la bande passante en bits/s, il existe des unités de mesure supérieures. La bande passante réseau est généralement exprimée en milliers de bits par seconde (kbits/s), millions de bits par seconde (Mbits/s), milliards de bits par seconde (Gbits/s) et billions de bits par seconde

(Tbits/s). 1

Unité de bande passante	Abréviation	Équivalences
Bits par seconde	bits/s	1 bit/s = unité fondamentale
Kilobits par seconde	kbits/s	1 kbits/s = 1,000 bps = 10^3 bits/s
Mégabits par seconde	Mbits/s	1 Mbits/s = 1,000,000 bps = 10^6 bits/s
Gigabits par seconde	Gbits/s	1 Gbits/s = 1,000,000,000 bps = 10^9 bits/s
Térabits par seconde	Tbits/s	1 Tbits/s = 1,000,000,000,000 bps = 10^{12} bits/s

Bien que les termes *bande passante* et *vitesse* soient souvent utilisés indifféremment, ils ne se rapportent pas exactement au même concept. On pourrait dire, par exemple, qu'une connexion T3 à 45 Mbits/s est plus rapide qu'une connexion T1 à 1,544 Mbits/s. Cependant, si une partie minime de leur capacité de transport de données est utilisée, chacune de ces connexions transportera les données à approximativement la même vitesse. De la même manière, un petit filet d'eau s'écoulera à la même vitesse dans un gros comme dans un petit tuyau. Il est donc plus précis de dire qu'une connexion T3 a une bande passante supérieure à celle d'une connexion T1. Cela vient de la capacité de la connexion T3 à transporter davantage d'informations en un temps donné, et non pas de sa vitesse supérieure.

La page suivante décrit les limitations de la bande passante.

2.2 Bande passante
2.2.4 Limitations

Cette page décrit les limitations de la bande passante.

La bande passante varie en fonction du type de média ainsi que des technologies LAN et WAN utilisées. La caractéristique physique du média entre en compte dans la différence. Les signaux peuvent circuler sur du fil de cuivre à paires torsadées, sur du câble coaxial, de la fibre optique ou par voie hertzienne. De ces différences physiques découlent des limitations fondamentales dans la capacité de transport des informations d'un média donné. Cependant, la bande passante proprement dite d'un réseau résulte d'une combinaison des médias physiques et des technologies choisis pour la signalisation et la détection des signaux du réseau.

Par exemple, les spécifications actuelles sur la physique du câble à paires torsadées non blindées (UTP) placent la limite théorique de la bande passante au-delà de 1 Gbit/s. Cependant, dans la pratique, la bande passante dépend de l'utilisation de 10BaseT, 100BaseTX ou 1000BaseTX Ethernet. La bande passante effective est déterminée par les méthodes de signalisation, les cartes réseau, ainsi que par les autres équipements de réseau choisis. Par conséquent, elle ne dépend pas uniquement des limitations du média.

La figure 1

Types de médias	Bande passante théorique maximale	Distance théorique maximale
Câble coaxial de 50 ohms (Ethernet 10Base2 ; Ethernet à câble fin)	10 Mbits/s	185 m
Câble coaxial de 50 ohms (Ethernet 10Base5 ; câble Ethernet épais)	10 Mbits/s	500 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 10BaseT)	10 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 100BaseTX)	100 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 1000BaseTX)	1000 Mbits/s	100 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	100 Mbits/s	220 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	1000 Mbits/s	220 m
Fibre optique multimode (50/125 m) (Ethernet 1000BaseSX)	1000 Mbits/s	550 m
Fibre optique monomode (9/125 m) (Ethernet 1000BaseLX)	1000 Mbits/s	5000 m

illustre certains types de médias de réseau ainsi que leurs limites en termes de distance et de bande passante.

La figure 2

Service WAN	Utilisateur type	Bande passante
	Individus	56 kbits/s = 0.056 Mbits/s
	Individus, télétravailleurs et petites entreprises	128 kbits/s to 6.1 Mbits/s = 0.128 Mbits/s to 6.1 Mbits/s
	Télétravailleurs et petites entreprises	128kbits/s = 0.128 Mbits/s
	Petites institutions (écoles) et WAN fiables	56 kbits/s à 44 736 Mbits/s (U.S.) ou 34 368 Mbits/s (Europe) = 0,056 Mbits/s à 44 736 Mbits/s (U.S.) ou 34 368 Mbits/s (Europe)
T1	Grandes organisations	1.544 Mbits/s
E1	Grandes organisations	2.048 Mbits/s
T3	Grandes organisations	44.736 Mbits/s
E3	Grandes organisations	34.368 Mbits/s
STM-0 (OC-1)	Compagnies de téléphone ; backbones des opérateurs Télécom	51.840 Mbits/s
STM-1	Compagnies de téléphone ; backbones des opérateurs Télécom	155.52 Mbits/s
STM-1 (OC-3)	Compagnies de téléphone ; backbones des opérateurs Télécom	155.251 Mbits/s
STM-3	Compagnies de téléphone ; backbones des opérateurs Télécom	466.56 Mbits/s
STM-16 (OC-48)	Compagnies de téléphone ; backbones des opérateurs Télécom	2.488320 Gbits/s

présente un récapitulatif des services de réseau étendu courants et de la bande passante associée à chacun d'eux.

La page suivante aborde le concept du débit.

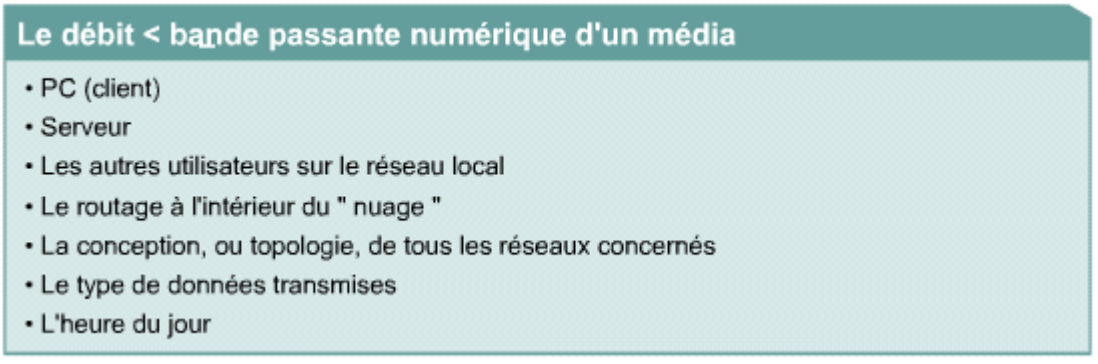
2.2 Bande passante

2.2.5 Débit

Cette page explique le concept du débit.

La bande passante est la mesure de la quantité d'informations pouvant transiter sur le réseau en un temps donné. Par conséquent, la quantité de bande passante disponible est un paramètre essentiel de la spécification du réseau. On peut construire un réseau local pour fournir 100 Mbits/s à chaque station de travail, mais cela ne veut pas dire que chaque utilisateur aura réellement la possibilité de transmettre 100 mégabits de données sur le réseau à chaque seconde d'utilisation. Cela ne peut être vrai que dans un cas de figure idéal.

Le terme débit se rapporte à la bande passante réelle mesurée, à une heure particulière de la journée, en empruntant des routes Internet particulières et lors de la transmission sur le réseau d'un ensemble de données spécifique. Malheureusement, pour de multiples raisons, le débit est souvent inférieur à la bande passante numérique maximale prise en charge par le média utilisé. Voici certains des facteurs déterminants pour le débit: 1


Le débit < bande passante numérique d'un média
• PC (client)
• Serveur
• Les autres utilisateurs sur le réseau local
• Le routage à l'intérieur du " nuage "
• La conception, ou topologie, de tous les réseaux concernés
• Le type de données transmises
• L'heure du jour

- Équipements d'interréseau
- Type de données transmises
- Topologie de réseau
- Nombre d'utilisateurs sur le réseau
- Ordinateur de l'utilisateur
- Ordinateur serveur,
- Conditions d'alimentation

La bande passante théorique d'un réseau est un facteur essentiel dans sa conception, du fait que la bande passante du réseau ne dépassera jamais les limites imposées par le média et par les technologies choisis. Cependant, il est tout aussi important pour un concepteur et un administrateur réseau de tenir compte des facteurs pouvant affecter le débit proprement dit. En mesurant régulièrement le débit, l'administrateur réseau pourra suivre les variations de performance du réseau ainsi que l'évolution des besoins de ses utilisateurs. Il paramètrera le réseau en conséquence.

La page suivante explique le calcul du taux de transfert des données.

2.2 Bande passante

2.2.6 Calcul du taux de transfert des données

Cette page présente la formule de calcul du taux de transfert des données.

Les concepteurs et administrateurs réseau sont souvent amenés à prendre des décisions à propos de la bande passante. Il peut s'agir par exemple de savoir s'il faut augmenter la taille de la connexion WAN afin de prendre en charge une nouvelle base de données, ou encore de déterminer si le backbone actuel du réseau local a une bande passante suffisante pour un programme de vidéo en continu. Il n'est pas toujours facile de trouver la réponse à des problèmes tels que ceux-ci, mais un simple calcul du taux de transfert des données est un excellent point de départ.

L'utilisation de la formule délai de transfert = taille de fichier / bande passante (D=T/BP) permet à l'administrateur du réseau d'évaluer plusieurs facteurs déterminants de la performance du réseau. Si l'on connaît la taille de fichier type pour une application donnée, il suffit de diviser la taille de fichier par la bande passante réseau pour obtenir une estimation du délai de temps de transfert le plus court pour le fichier. 1

Meilleur téléchargement

$$D = \frac{T}{BP}$$

Téléchargement type

$$D = \frac{T}{P}$$

BP	Bande passante théorique maximale de la liaison " la plus lente " entre l'hôte source et l'hôte de destination (mesurée en bits par seconde)
P	Débit effectif au moment du transfert (mesuré en bits par seconde)
D	Durée du transfert des fichiers (mesuré en secondes)
T	Taille de fichier en bits

Deux points importants doivent être pris en compte lors de ce calcul.

- Le résultat n'est qu'une estimation, parce que la taille du fichier n'inclut pas la surcharge due à l'encapsulation.
- On obtiendra un résultat pour un cas de figure idéal, or la bande passante disponible n'est presque jamais au maximum théorique de ses capacités pour le type de réseau. Il est possible d'obtenir une estimation plus précise en posant le débit plutôt que la bande passante dans l'équation.

Bien que le calcul du transfert de données soit assez simple, il faut veiller à utiliser les mêmes unités dans toute l'équation. En d'autres termes, si la bande passante est exprimée en mégabits par seconde (Mbits/s), la taille du fichier doit être elle aussi en mégabits, et pas en méga-octets (Mo). Étant donné que les tailles de fichier sont presque toujours exprimées en méga-octets, vous devrez multiplier par huit le nombre de méga-octets pour obtenir la valeur en mégabits.

Essayez de répondre à la question suivante, en utilisant la formule D=T/BP. Convertissez les unités de mesure comme il se doit.

Parmi les deux propositions suivantes, laquelle serait la plus rapide : envoyer le contenu d'une disquette pleine (1,44 Mo) sur une ligne RNIS ou envoyer le contenu d'un disque dur plein de 10 Go sur une ligne STM-16?

La page suivante compare les signaux analogiques et les signaux numériques.

2.2 Bande passante

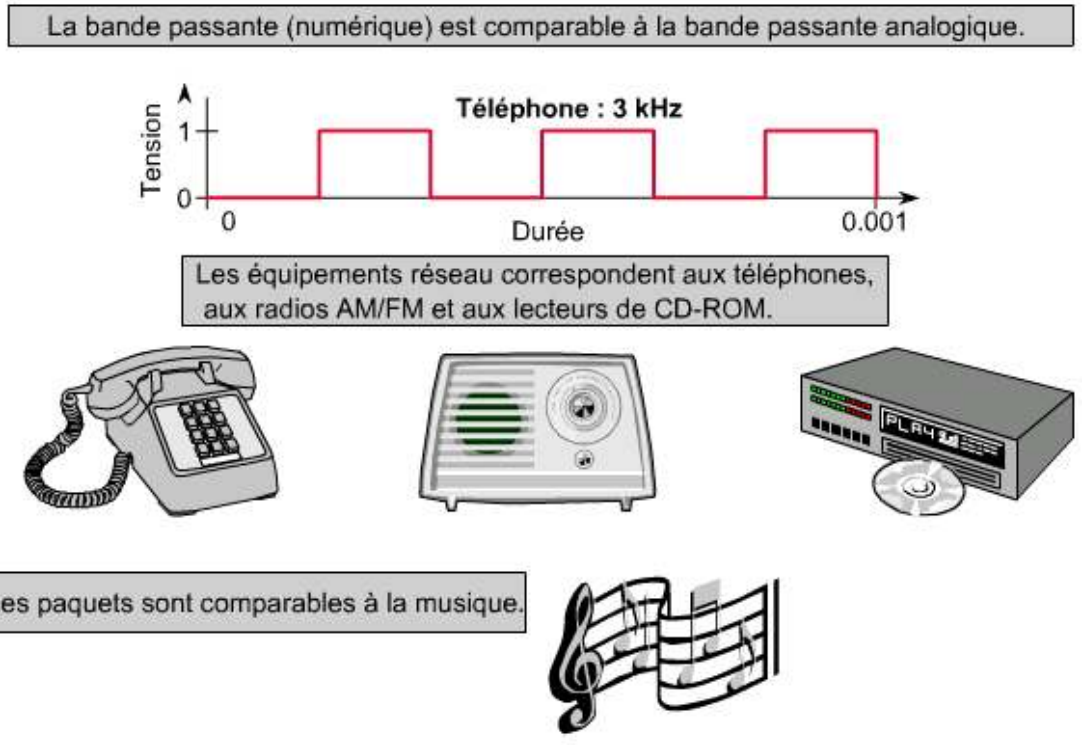
2.2.7 Numérique et analogique

Cette page expose les différences entre les signaux analogiques et les signaux numériques.

La majorité des transmissions radiophoniques, télévisuelles et téléphoniques s'effectue encore aujourd'hui au moyen d'ondes électromagnétiques empruntant la voie des airs ou des câbles. Ces ondes sont dites analogiques car elles ont la même forme que les ondes lumineuses et sonores produites par les émetteurs. Lorsque les ondes lumineuses et sonores changent de taille et de forme, le signal électrique qui transporte la transmission change

en proportion. En d'autres termes, les ondes électromagnétiques sont analogues aux ondes lumineuses et sonores.

La bande passante analogique est mesurée en fonction du taux d'occupation du spectre électromagnétique par chaque signal. L'unité de base de la bande passante analogique est le hertz (Hz), ou nombre de cycles par seconde. En général, comme pour la bande passante numérique, on utilise des multiples de cette unité de base de bande passante analogique. Les unités de mesure les plus usitées sont le kilohertz (KHz), le mégahertz (MHz) et le gigahertz (GHz). Ces unités sont utilisées pour décrire la fréquence des téléphones sans fil, qui fonctionnent habituellement à 900 MHz ou à 2,4 GHz. Elles servent aussi pour indiquer les fréquences des réseaux sans fil 802.11a et 802.11b, qui fonctionnent à 5 GHz et 2,4 GHz. 1


La bande passante (numérique) est comparable à la bande passante analogique.
Téléphone : 3 kHz
Tension
1
0
0
Durée
0.001
Les équipements réseau correspondent aux téléphones, aux radios AM/FM et aux lecteurs de CD-ROM.
Les paquets sont comparables à la musique.

Bien que les signaux analogiques soient capables de transporter une grande variété d'informations, ils n'offrent pas autant d'avantages que les transmissions numériques. Le signal vidéo analogique, du fait qu'il occupe une large plage de fréquences, ne peut pas être comprimé en une bande plus étroite. Par conséquent, si l'on ne dispose pas de la bande passante analogique nécessaire, il est impossible d'envoyer le signal.

Dans la signalisation numérique, toutes les informations, quel que soit leur type, sont envoyées sous forme de bits. La voix, la vidéo et les données sont convertis en flux de bits lors de leur préparation pour une transmission via des médias numériques. Ce type de transmission procure à la bande passante numérique un avantage décisif par rapport à la bande passante analogique. Il est possible d'envoyer des quantités illimitées d'informations via un canal numérique, même de faible bande passante. Quel que soit le temps nécessaire à leur transfert et à leur réassemblage, les informations numériques peuvent toujours être visualisées, écoutées ou traitées dans leur forme originale.

Il est important de comprendre les différences et les similitudes entre la bande passante numérique et la bande passante analogique. On rencontre régulièrement ces deux types de bandes dans le domaine des technologies de l'information. Cependant, étant donné que ce cours traite principalement de réseaux numériques, le terme «bande passante» sous-entendra «bande passante numérique».

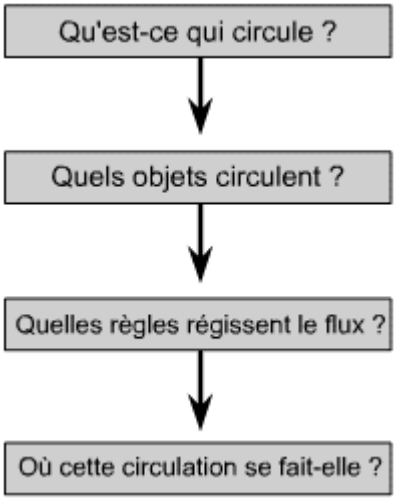
Cette leçon est terminée. La leçon suivante traite des modèles de réseau. La première page aborde le concept des couches.

2.3 Modèles de réseau

2.3.1 Utilisation des couches pour analyser les problèmes de flux

Cette page explique comment les couches sont utilisées pour décrire les communications entre les ordinateurs.

La figure 1



présente un ensemble de questions liées au flux, qui est défini comme le mouvement, à travers un système, d'objets physiques ou logiques. Ces questions montrent comment le concept de couches aide à décrire en détail le cheminement du flux. Ce processus peut s'appliquer à n'importe quel type de flux, qu'il s'agisse du flux du trafic sur un réseau routier ou du flux de données au sein d'un réseau informatique. La figure 2

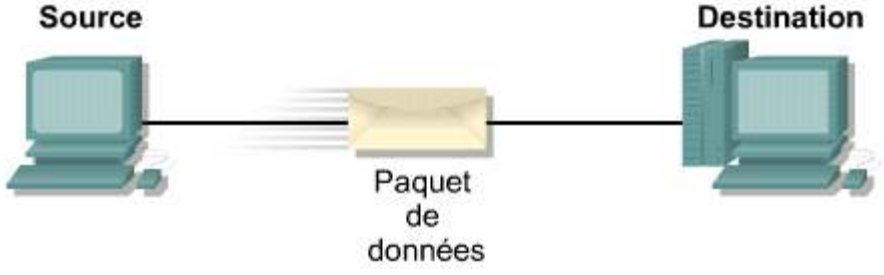
Réseau	Ce qui circule	Sous quelle forme	Règles	Où ?
Eau	Eau	Chaude ; froide ; potable ; eau usée/égout	Règles d'accès (robinets) ; chasse d'eau ; ne pas jeter certains produits	Tuyaux
Autoroute	Véhicules	Camions, voitures, motocyclettes	Règles de circulation et règles de politesse	Routes et autoroutes
Courrier postal	Objets	Lettres (informations écrites) ; colis	Règles d'emballage et d'affranchissement	Boîtes postales, boîtes aux lettres, bureaux, camions, avions, facteurs
Téléphone	Informations	Langues parlées	Règles d'accès au téléphone et règles de politesse	Fils du système téléphonique, ondes électromagnétiques, etc.

montre divers exemples de flux et de façons de décomposer le cheminement du flux en détails ou couches.

Une conversation entre deux personnes constitue un champ idéal pour tester l'approche en couches afin d'analyser des flux d'informations. Lors d'une conversation, chaque personne qui souhaite communiquer commence par avoir une idée. Elle prend ensuite une décision sur la façon de communiquer cette idée correctement. Par exemple, une personne pourra choisir de parler, chanter ou crier dans une langue donnée. Enfin l'idée est exprimée. La personne émet le son qui transporte le message.

Ce processus peut être décomposé en couches distinctes applicables à toutes les conversations. La couche supérieure correspond à l'idée qui sera communiquée. La couche du milieu à la décision, ou à la façon dont l'idée doit être communiquée. La couche inférieure correspond à la création de sons pour transporter la communication.

La même méthode de subdivision en couches nous permet de définir comment un réseau informatique distribue des informations entre une source et une destination. Lorsque des ordinateurs envoient des informations sur un réseau, toutes les communications doivent provenir d'une source et se diriger vers une destination. 3



On appelle généralement données, ou paquet, les informations qui transitent sur un réseau. Un paquet est constitué d'une unité d'informations groupées de manière logique qui circule entre des ordinateurs. Lorsque les données traversent les couches, chaque couche ajoute des informations supplémentaires qui permettent une communication efficace avec la couche correspondante de l'autre ordinateur.

Les modèles OSI et TCP/IP comportent des couches qui spécifient comment les données doivent être communiquées d'un ordinateur à l'autre. Les modèles diffèrent en fonction du nombre et de la fonction des couches. Cependant, chaque modèle peut être utilisé pour décrire et préciser le flux d'informations entre une source et une destination.

La page suivante explique comment les couches sont utilisées pour décrire les communications des données.

2.3 Modèles de réseau

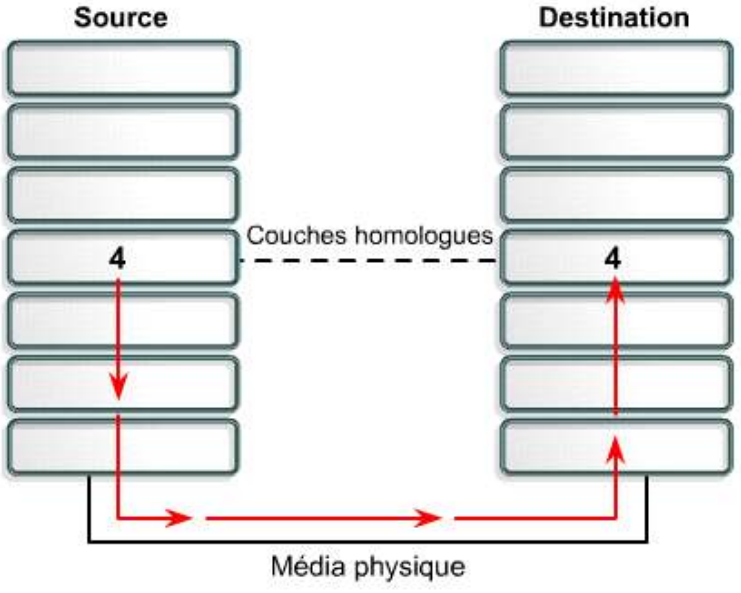
2.3.2 Utilisation de couches pour décrire la communication des données

Cette page décrit l'importance des couches dans les communications des données.

Pour que des paquets de données puissent se rendre d'un ordinateur source à un ordinateur de destination sur un réseau, il est important que toutes les unités du réseau communiquent selon la même langue ou dans le même protocole. Un protocole consiste en un ensemble de règles qui augmentent l'efficacité des communications au sein d'un réseau. Par exemple, lorsqu'ils pilotent un avion, les pilotes obéissent à des règles très précises pour communiquer d'un appareil à l'autre ou d'un appareil à la tour de contrôle.

Un protocole de communications de données est un ensemble de règles, ou convention, qui détermine le format et la transmission des données.

La couche 4 de l'ordinateur source communique avec la couche 4 de l'ordinateur de destination. 1



Les règles et conventions utilisées pour cette couche sont appelées protocole de couche 4. Il est important de se souvenir que les protocoles préparent les données de façon linéaire. Un protocole d'une couche effectue un certain nombre d'opérations sur les données lorsqu'il les prépare pour les envoyer sur le réseau. Les données sont ensuite transmises à la couche suivante, où un autre protocole effectue une série d'opérations différentes.

Une fois que le paquet a été envoyé vers sa destination, les protocoles annulent la constitution du paquet qui a été effectuée côté source. L'opération est effectuée à rebours. Les protocoles de chaque couche de destination rétablissent la forme originale des informations, pour que l'application puisse lire correctement les données.

La page suivante explique le modèle OSI.

2.3 Modèles de réseau

2.3.3 Modèle OSI

Cette page explique comment et pourquoi le modèle OSI a été développé.

À ses débuts, le développement des réseaux était désorganisé à de nombreux égards. Le début des années 1980 a été marqué par une croissance exceptionnelle du nombre et de la taille des réseaux. Pour profiter des avantages de l'utilisation de la technologie réseau, les sociétés se mirent à installer et à étendre des réseaux, à un rythme presque aussi rapide que l'introduction des nouvelles technologies.

Vers le milieu des années 80, ces sociétés commencèrent à rencontrer des problèmes, justement en raison de cette extension rapide. Tout comme il est difficile pour les gens qui ne parlent pas la même langue de communiquer, il devenait difficile pour des réseaux qui utilisent des spécifications et des implémentations différentes d'échanger des informations. Les sociétés qui développaient des solutions de réseau privé ou propriétaire furent confrontées au même problème. Le terme « propriétaire » signifie ici qu'une entreprise ou un petit groupe d'entreprises contrôle entièrement l'utilisation de la technologie. Les technologies réseau qui suivaient strictement des règles propriétaires ne pouvaient pas communiquer avec des technologies qui respectaient des règles propriétaires différentes.

Pour résoudre le problème de l'incompatibilité des réseaux, l'OSI (International Organization for Standardization) examina les modèles réseau tels que DECnet (Digital Equipment Corporation net), SNA (Systems Network Architecture) et TCP/IP afin de trouver un ensemble de règles applicable de façon générale à

tous les réseaux. Sur la base de ces recherches, l'ISO a mis au point un modèle de réseau pour aider les fournisseurs à créer des réseaux compatibles avec d'autres réseaux.

Le modèle de référence OSI (Open System Interconnection) publié en 1984 fut le modèle descriptif de réseau créé par l'ISO. Ce modèle propose aux fournisseurs un ensemble de normes assurant une compatibilité et une interopérabilité accrues entre divers types de technologies réseau produites par de nombreuses entreprises à travers le monde. [1]



Avantages du modèle OSI :
- Il réduit la complexité.
- Il uniformise les interfaces.
- Il facilite la conception modulaire.
- Il assure l'interopérabilité de la technologie.
- Il accélère l'évolution.
- Il simplifie l'enseignement et l'acquisition des connaissances.

Le modèle de référence OSI s'est imposé comme le principal modèle pour les communications réseau. Bien qu'il existe d'autres modèles, la plupart des constructeurs de réseau se fondent sur le modèle de référence OSI pour la conception de leurs produits. Cela est particulièrement vrai lorsqu'ils souhaitent éduquer les utilisateurs à l'utilisation de leurs produits. Ce modèle est considéré comme le meilleur outil disponible pour décrire l'envoi et la réception de données sur un réseau.

Dans l'activité de média interactive, les étudiants seront en mesure d'identifier les avantages du modèle OSI.

La page suivante décrit les différentes couches du modèle OSI.

Activité de média interactive

Case à cocher: Avantages du modèle OSI

À la fin de cette activité, l'étudiant doit être en mesure d'identifier les avantages du modèle OSI.

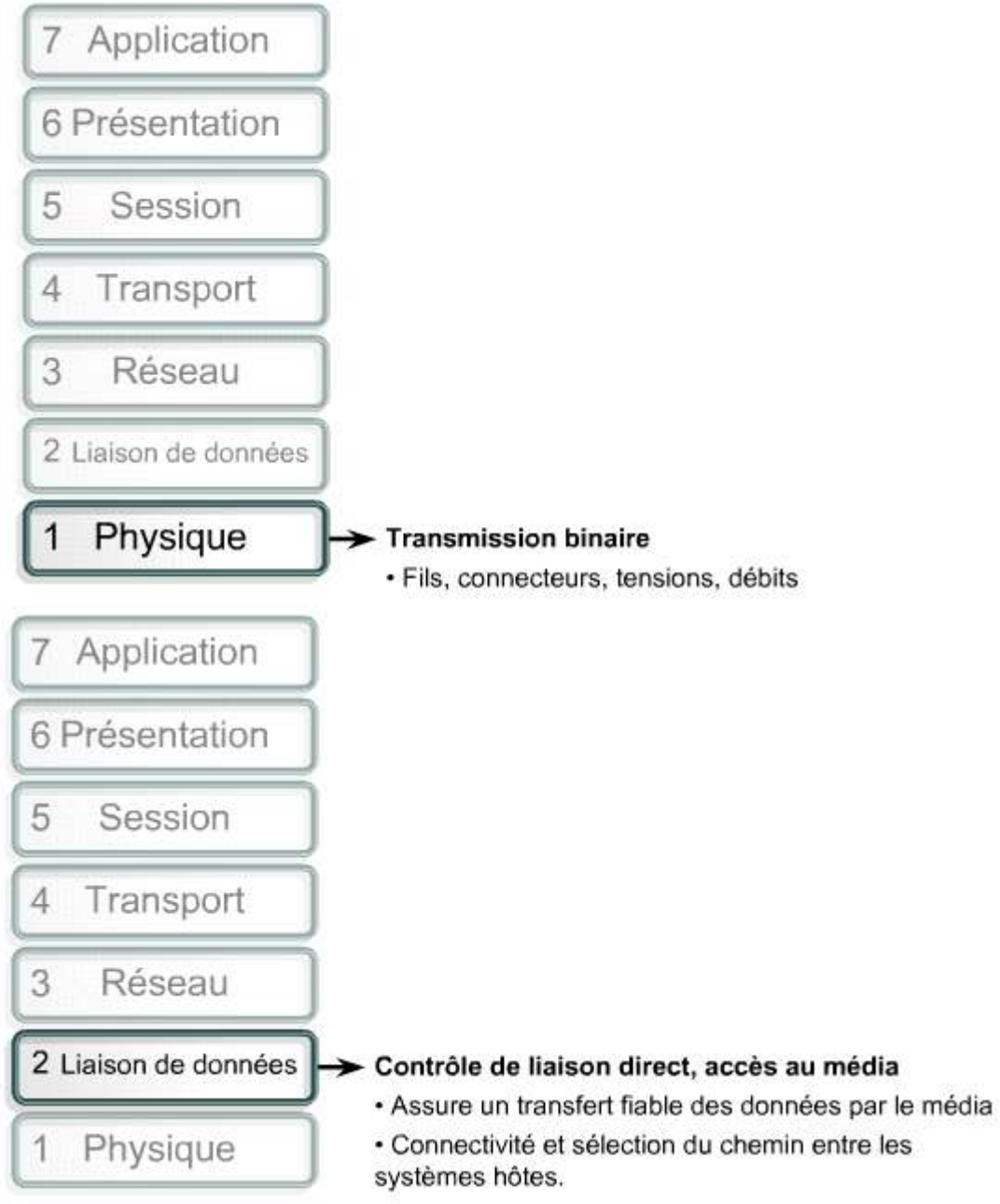
2.3 Modèles de réseau

2.3.4 Couches OSI

Cette page présente chacune des sept couches du modèle OSI.

Le modèle de référence OSI constitue un cadre qui aide à comprendre comment les informations circulent dans un réseau. Ce modèle explique comment les paquets transitent à travers les différentes couches vers un autre équipement du réseau, même si l'émetteur et le destinataire utilisent des types de média réseau différents.

Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. 1 – 7





Adresse réseau et détermination du meilleur chemin

- Assure un transfert fiable des données par le média
- Connectivité et sélection du chemin entre les systèmes hôtes.
- Adressage logique
- Acheminement au mieux



Connexions de bout en bout

- Concerne les problèmes de transport entre les hôtes
- Fiabilité du transport des données
- Établissement, maintien et terminaison des circuits virtuels
- Détection des pannes et reprise du contrôle du flux d'information

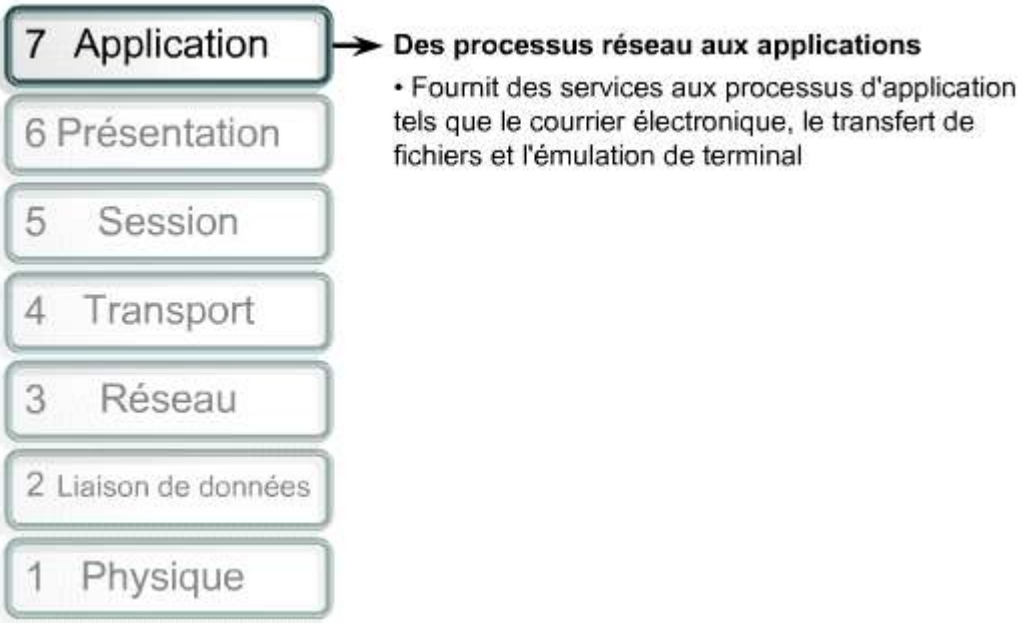


Communication entre les hôtes

- Établit, gère et ferme les sessions entre les applications

Représentation des données

- Lisibilité des données pour le système de destination
- Format des données
- Structures des données
- Négocie la syntaxe de transfert des données pour la couche application


7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique
Des processus réseau aux applications
• Fournit des services aux processus d'application tels que le courrier électronique, le transfert de fichiers et l'émulation de terminal

Le découpage du réseau en sept couches présente les avantages suivants:

- Il permet de diviser les communications sur le réseau en éléments plus petits et plus gérables.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multiconstructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Les modifications apportées à une couche n'affectent pas les autres couches.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.

Dans l'activité de média interactive suivantes, les étudiants vont identifier les sept couches du modèle OSI.

La page suivante décrit les communications point-à-point à travers le modèle OSI.

Activité de média interactive

Glisser-Positionner: Les sept couches du modèle OSI

À la fin de cette activité, l'étudiant doit être en mesure d'identifier certaines des fonctions des sept couches OSI.

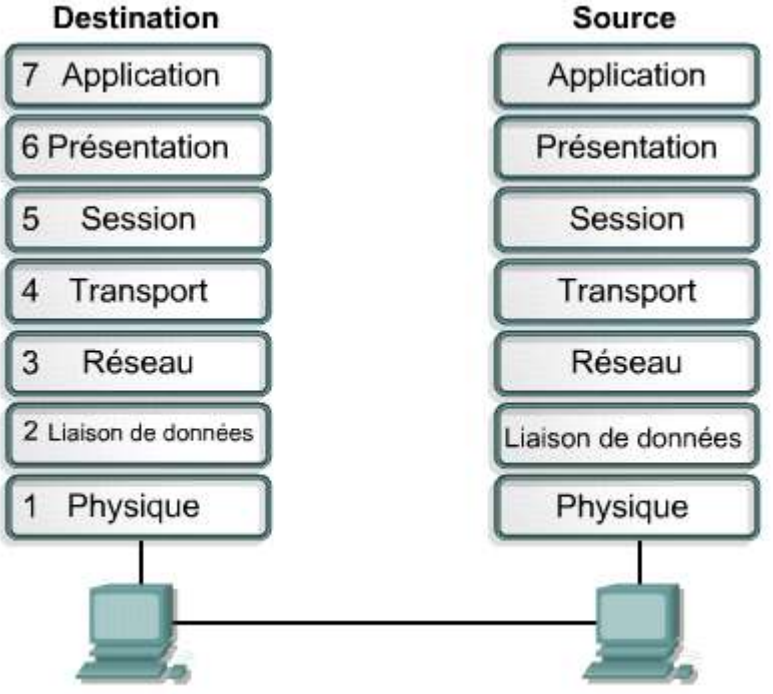
2.3 Modèles de réseau

2.3.5 Communications d'égal à égal

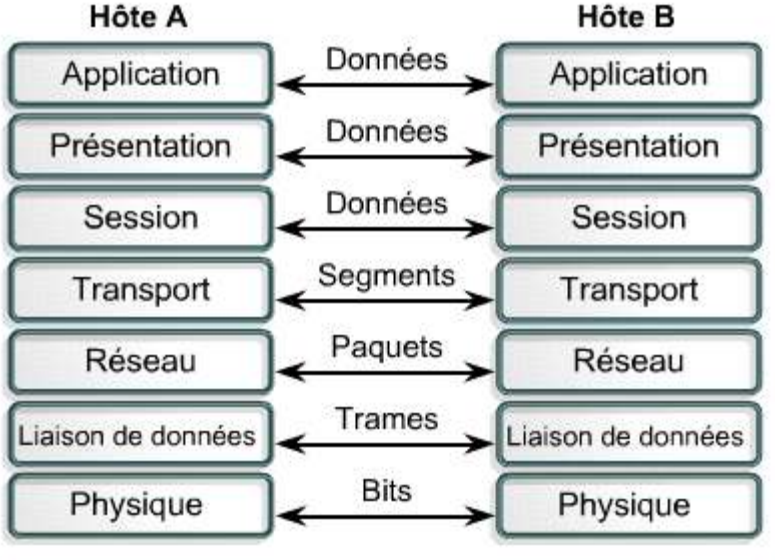
Cette page explique le concept de communications d'égal à égal.

Afin de permettre l'acheminement des données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI au niveau de l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination. Cette forme de communication est appelée communication d'égal à égal. Au cours de ce processus, les protocoles de chaque couche s'échangent des informations, appelées unités de données de protocole (PDU). Chaque couche de communication, sur l'ordinateur source, communique avec l'unité de

données de protocole propre à une couche, ainsi qu'avec la couche correspondante sur l'ordinateur de destination, comme l'illustre la figure 1.



Dans un réseau, les paquets de données proviennent d'une source et sont acheminés vers une destination. Chaque couche dépend de la fonction de service de la couche OSI sous-jacente. Pour fournir ce service, la couche inférieure utilise l'encapsulation pour placer les PDU de la couche supérieure dans son champ de données. Elle ajoute ensuite les en-têtes et les en-queues de PDU nécessaires à l'exécution de sa fonction. Par la suite, à mesure que les données traversent les couches du modèle OSI, d'autres en-têtes et en-queues sont ajoutés. Dès que les couches 7, 6 et 5 ont ajouté leurs informations, la couche 4 en ajoute d'autres. Ce regroupement des données, ou unité de données de protocole de couche 4, est appelé segment. 2



Ainsi, la couche réseau fournit un service à la couche transport, qui présente les données au sous-système de l'interréseau. La couche réseau est chargée de déplacer les données dans l'interréseau. Pour ce faire, elle encapsule les données et leur annexe un en-tête de manière à créer un paquet (soit la PDU de couche 3). L'en-tête contient les informations requises pour effectuer le transfert, notamment les adresses logiques de source et de destination.

La couche liaison de données fournit un service à la couche réseau. Elle encapsule le paquet de la couche réseau dans une trame (le PDU de couche 2). L'en-tête de trame contient les informations (par exemple des adresses physiques) nécessaires à l'exécution des fonctions de liaison de données. La couche liaison de données fournit donc un service à la couche réseau en encapsulant les informations de couche réseau dans une trame.

La couche physique fournit également un service à la couche liaison de données. Elle code la trame de liaison en une série de uns et de zéros (bits) en vue de la transmettre sur un média (habituellement un fil) dans la couche 1.

La page suivante décrit le modèle de référence TCP/IP.

2.3 Modèles de réseau

2.3.6 Modèle TCP/IP

Cette page décrit le modèle de référence TCP/IP, qui est la norme historique et technique d'Internet.

Le ministère américain de la Défense a créé le modèle de référence TCP/IP parce qu'il avait besoin de concevoir un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire. Dans un monde connecté par différents types de médias de communication tels que les fils de cuivre, micro-ondes, fibres optiques et liaisons satellite, le ministère de la défense souhaitait une transmission de paquets capable d'aboutir à coup sûr et sous n'importe quelle condition. Ce problème de conception extrêmement ambitieux a conduit à la création du modèle TCP/IP.

Contrairement aux technologies réseau propriétaires mentionnées précédemment, TCP/IP a été développé en tant que norme ouverte. Cela voulait dire que n'importe qui pouvait utiliser TCP/IP. Cela contribua à accélérer le développement de TCP/IP en tant que norme.

Le modèle TCP/IP comporte les quatre couches suivantes:

- La couche application
- La couche transport
- La couche Internet
- La couche d'accès au réseau 1



Bien que certaines couches du modèle TCP/IP aient le même nom que les couches du modèle OSI, elles ne correspondent pas exactement. Il est à noter que la couche application assure différentes fonctions dans chaque modèle.

Les concepteurs du modèle TCP/IP estimaient que la couche application devait inclure les détails des couches session et présentation OSI. Ils ont donc créé une couche application qui gère les questions de représentation, le code et le contrôle du dialogue.

La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (*Transmission Control Protocol - protocole de contrôle de transmission*), fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.

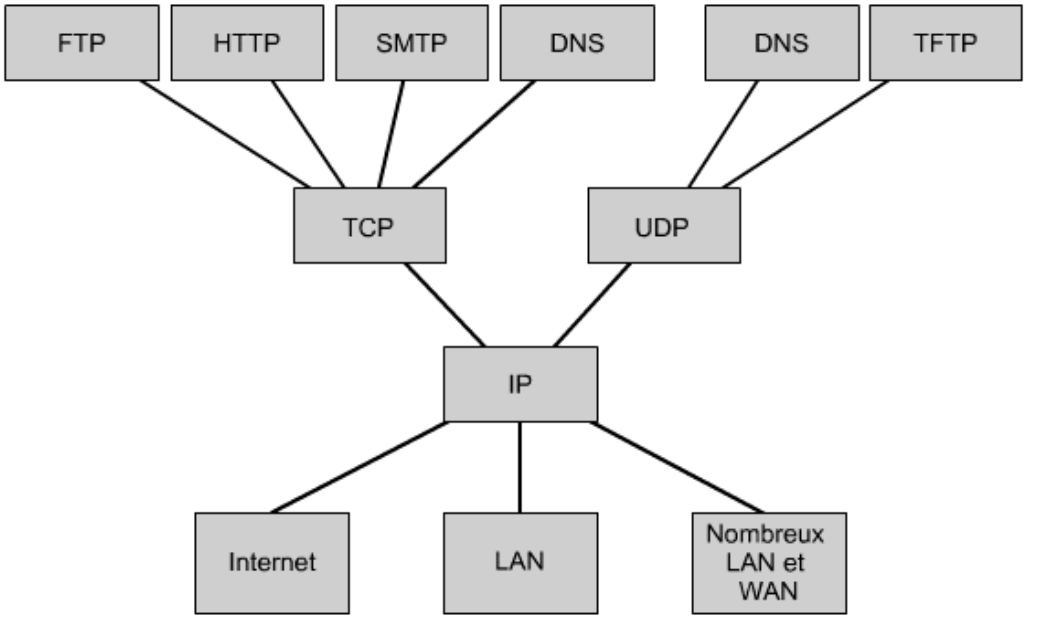
Le protocole TCP est orienté connexion. Il maintient un dialogue entre l'ordinateur source et l'ordinateur de destination pendant qu'il prépare les informations de couche application en unités, appelées segments. Un protocole orienté connexion ne signifie pas qu'il existe un circuit entre les ordinateurs en communication. Ce type de fonctionnement indique qu'il y a un échange de segments de couche 4 entre les deux ordinateurs hôtes afin de confirmer l'existence logique de la connexion pendant un certain temps.

L'objectif de la couche Internet est de diviser les segments TCP en paquets et de les envoyer depuis n'importe quel réseau. Les paquets arrivent au réseau de destination indépendamment du chemin qu'ils ont emprunté pour y parvenir. Le protocole qui régit cette couche est appelée protocole IP (Internet Protocol). La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

La relation entre IP et TCP est essentielle. Chaque protocole joue un rôle particulier : IP pointe le chemin pour les paquets, tandis que TCP assure un transport fiable.

Le nom de la couche d'accès au réseau a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche concerne tous les composants, à la fois physiques et logiques, qui sont nécessaires pour créer une liaison physique. Elle comprend les détails sur les technologies de réseau, ainsi que tous ceux qui concernent les couches physique et liaison de données du modèle OSI.

La figure 2



présente certains protocoles communs spécifiés par les couches du modèle de référence TCP/IP. Certains des protocoles de couche application les plus courants sont:

- FTP (*File Transfer Protocol*)
- HTTP (*HyperText Transfer Protocol*)
- SMTP (*Simple Mail Transfer Protocol*)
- DNS (*Domain Name System*)
- TFTP (*Trivial File Transfer Protocol*)

Les protocoles les plus courants de la couche transport sont notamment:

- TCP (*Transport Control Protocol*)
- UDP (*User Datagram Protocol*)

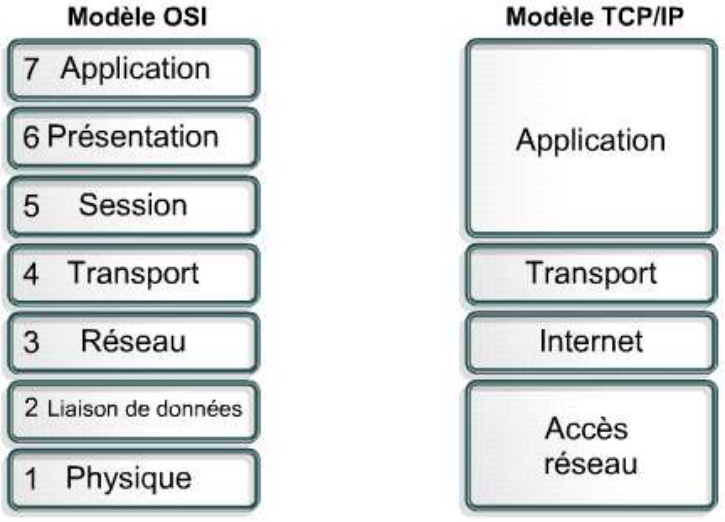
Le protocole principal de la couche Internet est:

- IP (*Internet Protocol*)

La couche d'accès réseau se rapporte à toute technologie particulière utilisée sur un réseau spécifique.

Quels que soient les services d'application réseau fournis et les protocoles de transport utilisés, il n'y a qu'un protocole Internet : IP. Il s'agit là d'un choix délibéré dans la conception. IP est un protocole universel qui permet à tout ordinateur de communiquer en tout temps et en tout lieu.

En comparant le modèle OSI au modèle TCP/IP, vous remarquerez des similitudes et des différences.



Les similitudes sont les suivantes:

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services très différents.
- Tous deux comportent des couches réseau et transport comparables.
- Les professionnels des réseaux doivent connaître ces deux modèles.
- Tous deux supposent que les paquets sont commutés. Cela signifie que chaque paquet peut prendre des chemins différents pour atteindre une même destination. Cela est différent des réseaux à commutation de circuits, où tous les paquets prennent le même chemin.

Les différences sont les suivantes:

- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe la couche physique et la couche liaison de données du modèle OSI dans la couche d'accès réseau.
- TCP/IP paraît plus simple, car il comporte moins de couches.
- Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles. En revanche, les réseaux ne sont généralement pas architecturés autour du protocole OSI, même si le modèle OSI puisse être utilisé comme guide.

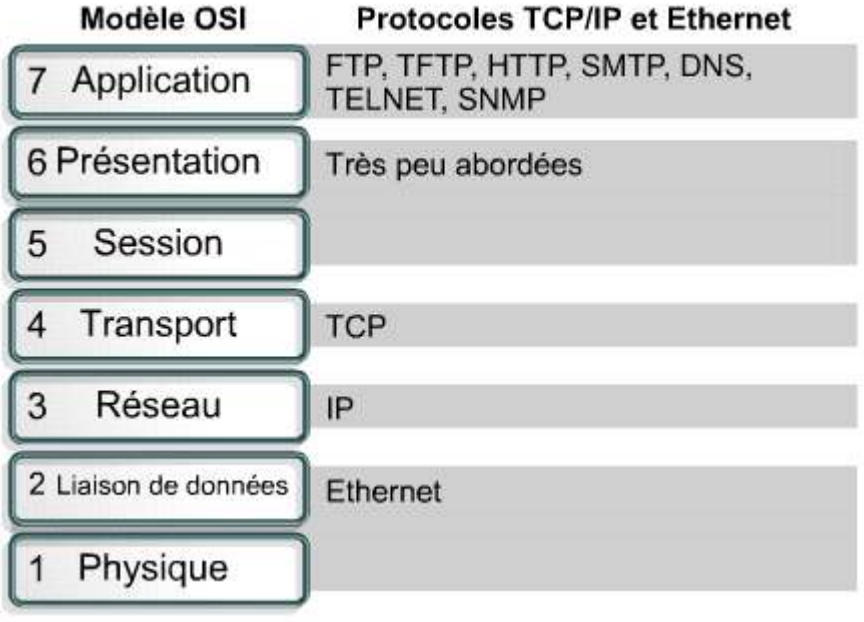
Bien que les protocoles TCP/IP constituent les normes sur lesquelles repose Internet, le modèle OSI a été choisi pour les raisons suivantes dans le cadre de ce cursus:

- Il s'agit d'une norme générique et indépendante du protocole.
- Ce modèle comporte davantage de détails, ce qui le rend plus utile pour l'enseignement et l'étude.
- Cette richesse de détails peut également s'avérer fort utile au moment du dépannage.

L'opinion de nombreux professionnels des réseaux diffère quant au modèle à utiliser. En raison des tendances de l'industrie, il est nécessaire de se familiariser avec les deux. Tout au long de ce cursus, il sera fait référence aux modèles OSI et TCP/IP. L'accent sera mis sur les points suivants:

- TCP en tant que protocole de couche 4 OSI
- IP en tant que protocole de couche 3 OSI
- Ethernet en tant que technologie de couche 2 et de couche 1

Souvenez-vous qu'il existe une différence entre un modèle et un protocole réel utilisé dans les réseaux. Le modèle OSI est utilisé pour décrire les protocoles TCP/IP. 4



Les étudiants identifieront les différences entre le modèle OSI et le modèle TCP/IP dans l'activité de TP.

Dans l'activité de média interactive, les étudiants seront en mesure d'identifier les couches du modèle de référence TCP/IP.

La page suivante explique le processus d'encapsulation.

Activité de TP

Exercice: Modèle OSI et modèle TCP/IP

Au cours de ce TP, l'étudiant va découvrir les quatre couches du modèle TCP/IP et les sept couches du modèle OSI correspondant aux quatre couches du modèle TCP/IP.

Activité de média interactive

Glisser-Positionner: Modèle TCP/IP du DoD

À la fin de cette activité, l'étudiant doit être en mesure d'identifier les couches du modèle TCP/IP.

2.3 Modèles de réseau

2.3.7 Processus d'encapsulation détaillé

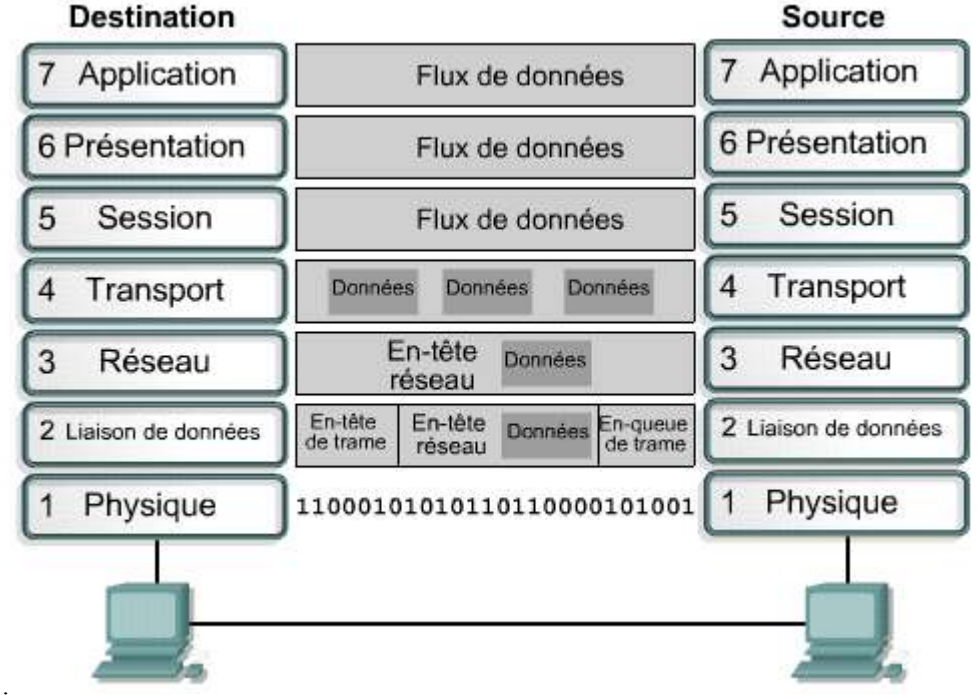
Cette page décrit le processus d'encapsulation.

Dans un réseau, toutes les communications proviennent d'une source et sont acheminées vers une destination. On appelle données, ou paquets de données, les informations qui transitent sur un réseau. Si un ordinateur (hôte

A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation.

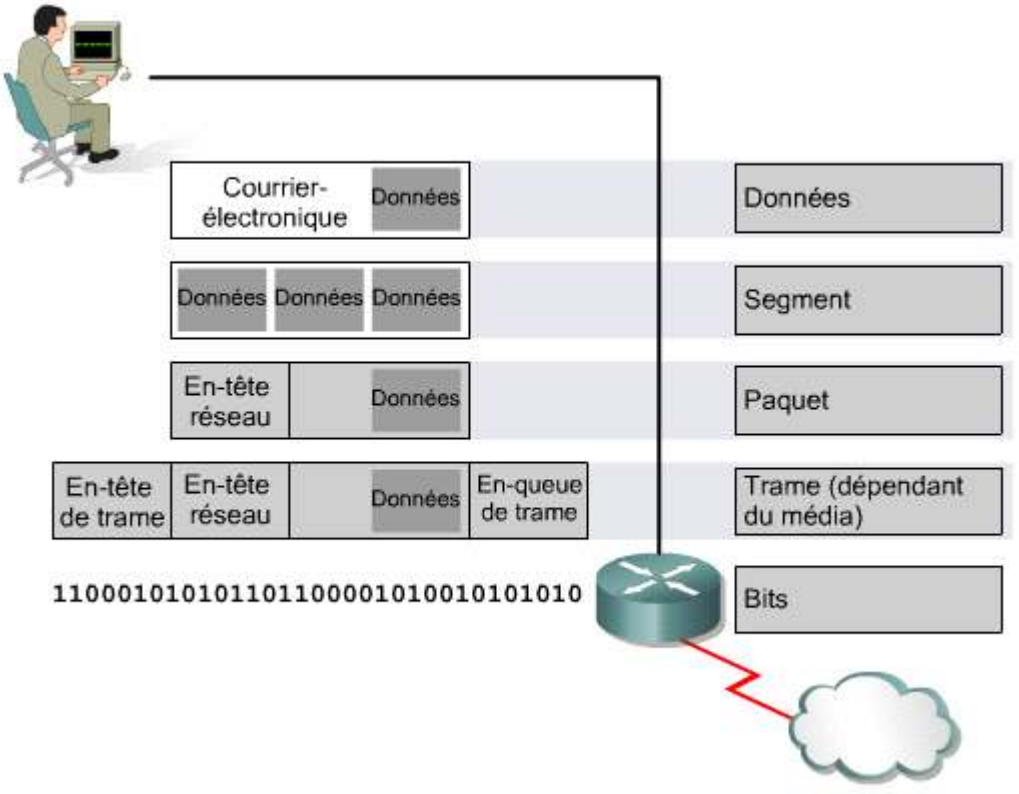
Ce processus conditionne les données en leur ajoutant des informations relatives au protocole avant de les transmettre sur le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des en-queues et d'autres informations.

Pour comprendre comment se déroule l'encapsulation, examinons la manière dont les données traversent les couches, comme l'illustre la figure 1



.

Les données qui sont envoyées par l'ordinateur source traversent la couche application et les autres couches. Comme vous pouvez le constater, la présentation et le flux des données échangées subissent des changements au fur et à mesure que les réseaux fournissent leurs services aux utilisateurs finaux. Comme le montre la figure 2,



les réseaux doivent effectuer les cinq étapes de conversion ci-dessous afin d'encapsuler les données:

1. **Construction des données –** Lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'interréseau.
2. **Préparation des données pour le transport de bout en bout –** Les données sont préparées pour le transport interréseau En utilisant des segments, la fonction de transport s'assure que les systèmes hôtes situés à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.
3. **Ajout de l'adresse IP du réseau à l'en-tête –** Les données sont organisées en paquets, ou datagrammes, contenant un en-tête de paquet constitué des adresses logiques d'origine et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.
4. **Ajout de l'en-tête et de l'en-queue de la couche de liaison de données –** Chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la prochaine unité réseau directement connectée dans la liaison. Chaque unité se trouvant sur le chemin réseau choisi doit effectuer un verrouillage de trame pour pouvoir se connecter à la prochaine unité.
5. **Conversion en bits pour la transmission –** La trame doit être convertie en une série de uns et de zéros (bits) pour la transmission sur le média. Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'interréseau physique, le média peut varier. Ainsi, le message électronique peut provenir d'un réseau local, traverser le backbone d'un campus, sortir par une liaison WAN pour atteindre sa destination sur un autre LAN éloigné.

L'activité de TP fournit une vue d'ensemble détaillée du modèle OSI.

Dans le cadre de l'activité de média interactive, les étudiants doivent effectuer un organigramme du processus d'encapsulation.

Cette leçon est terminée. La page suivante résume les principaux points du module.

Activité de TP

Exercice: Caractéristiques du modèle OSI et équipements associés

Dans ce TP, l'étudiant va apprendre les sept couches du modèle OSI ainsi que les caractéristiques, fonctions et mots clés liés à chaque couche.

Résumé

Cette page résume les sujets traités dans ce module.

Les réseaux informatiques ont été développés en réponse à des besoins informatiques, commerciaux et gouvernementaux. L'application de normes aux fonctions du réseau a donné lieu à un ensemble de directives afin de créer des logiciels et des matériels pour le réseau, et a assuré la compatibilité entre les équipements de différentes sociétés. Les informations pouvaient ainsi circuler au sein de la société et d'une entreprise à l'autre.

Les équipements de réseau, tels que les répéteurs, concentrateurs, ponts, commutateurs et routeurs interconnectent les équipements hôtes pour leur permettre de communiquer. Les protocoles fournissent un ensemble de règles pour la communication.

La topologie physique d'un réseau spécifie la disposition effective des fils ou médias. La topologie physique définit comment les équipements hôtes accèdent au média. Les topologies physiques couramment utilisées sont la topologie en bus, la topologie en anneau, la topologie en étoile, la topologie en étoile étendue, la topologie hiérarchique et la topologie maillée. Les deux types de topologie logique les plus courants sont le broadcast et le passage de jeton.

Un réseau local (LAN) est conçu pour fonctionner dans une zone géographique limitée. Les réseaux locaux permettent un accès multiple à des médias à large bande passante, assurent un contrôle privé du réseau sous administration locale ainsi qu'une connectivité continue aux services locaux, et connectent physiquement les services adjacents.

Un réseau étendu (WAN) est conçu pour fonctionner sur une zone géographique étendue. Les réseaux étendus permettent l'accès sur des interfaces série fonctionnant à basse vitesse, fournissent une connectivité continue et intermittente et raccordent les équipements disséminés sur des zones étendues.

Un réseau métropolitain (MAN) est un réseau qui s'étend à une zone métropolitaine telle qu'une ville ou une zone de banlieue. Un réseau MAN consiste habituellement en deux réseaux LAN au moins, situés dans une zone géographique commune.

Un réseau de stockage (SAN) est un réseau à haute performance dédié qui sert à transférer des données entre des serveurs et des ressources de stockage. Un réseau SAN fournit des performances système améliorées, il est évolutif et il intègre la tolérance aux sinistres.

Un réseau privé virtuel (VPN) est un réseau privé construit au sein d'une infrastructure de réseau publique. Les VPN d'accès, d'intranet et d'extranet sont les trois principaux types de VPN. Les VPN d'accès fournissent aux utilisateurs mobiles et de petits bureaux/bureaux à domicile (SOHO), l'accès distant à un intranet ou à un extranet. Les intranets sont uniquement disponibles pour les utilisateurs qui ont des privilèges d'accès au réseau interne de l'organisation. Les extranets sont conçus pour délivrer aux utilisateurs et entreprises externes des applications et des services qui sont basés sur intranet.

On appelle bande passante la quantité d'informations pouvant transiter sur une connexion réseau en un temps donné. La bande passante du réseau est généralement exprimée en milliers de bits par seconde (kbits/s), millions de bits par seconde (Mbits/s), milliards de bits par second (Gbits/s) et billions de bits par seconde

(Tbits/s). La bande passante théorique d'un réseau est un facteur essentiel dans la conception d'un réseau. Si l'on connaît la bande passante théorique d'un réseau, la formule D=T/BD (délai de transfert = taille de fichier / bande passante) peut être utilisée pour calculer le délai de transfert potentiel. Cependant, la bande passante effective, appelée débit, est affectée par de multiples facteurs tels que les équipements de réseau et la topologie utilisée, le type de données, le nombre d'utilisateurs, le matériel et les conditions d'alimentation.

Les données peuvent être codées sur des signaux analogiques ou numériques. La bande passante analogique est une mesure du taux d'occupation par chaque signal du spectre électromagnétique. Par exemple, le signal vidéo analogique qui nécessite une large plage de fréquences pour sa transmission ne peut pas être comprimé dans une bande plus étroite. Par conséquent, si la bande passante analogique nécessaire n'est pas disponible, il est impossible d'envoyer le signal. Dans la signalisation numérique, toutes les informations sont envoyées sous forme de bits, et ce, quel que soit leur type. Il est possible d'envoyer des quantités illimitées d'informations sur un canal numérique de faible bande passante.

Le concept de couches est utilisé pour décrire la communication d'un ordinateur à l'autre. Le découpage du réseau en couches présente les avantages suivants:

- Il réduit la complexité.
- Il uniformise les interfaces.
- Il facilite la conception modulaire.
- Il garantit l'interopérabilité.
- Il accélère l'évolution.
- Il simplifie l'enseignement et l'acquisition des connaissances.

Les modèles réseau OSI (Open System Interconnection) et le TCP/IP sont des modèles en couches. Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Application, présentation, session, transport, réseau, liaison de données et physique Le modèle TCP/IP comporte les quatre couches suivantes : application, transport, Internet et accès réseau

Bien que certaines couches du modèle TCP/IP aient le même nom que les couches du modèle OSI, les couches des deux modèles ne correspondent pas de façon exacte. La couche application TCP/IP est équivalente aux couches application, présentation et session de l'OSI. Le modèle TCP/IP regroupe la couche physique et la couche liaison de données du modèle OSI dans la couche d'accès réseau.

Quel que soit le modèle appliqué, les couches réseau effectuent les cinq étapes de conversion ci-dessous afin d'encapsuler et de transmettre les données:

1. Les images et le texte sont convertis en données.
2. Les données sont regroupées en segments.
3. Le segment de données est encapsulé dans un paquet avec les adresses source et de destination.
4. Le paquet est ensuite encapsulé dans une trame avec l'adresse MAC source en plus de celle du prochain équipement directement connecté.
5. La trame est convertie en une série de uns et de zéros (bits) pour la transmission sur le média.

Résumé

• Les cartes réseau, les répéteurs, les concentrateurs, les ponts, les commutateurs et les routeurs sont des équipements réseau courants.

• On rencontre couramment les types de réseau suivants : LAN, WAN, MAN, SAN et VPN.

• La bande passante est définie comme la quantité d'informations pouvant transiter sur une connexion réseau en un temps donné.

• Les deux modèles réseau les plus connus sont : le modèle de référence OSI et le modèle TCP/IP.

3-Médias réseau

Vue d'ensemble

Le câble de cuivre est utilisé dans la plupart des réseaux locaux. Les nombreux modèles disponibles présentent chacun des avantages et des inconvénients. Le choix d'un câblage adapté est essentiel au bon fonctionnement d'un réseau. Comme le cuivre utilise le courant électrique pour transmettre des informations, il est important de comprendre certaines notions de base en électricité.

La fibre optique est le média le plus couramment utilisé pour assurer les transmissions point-à-point, plus longues et à haut débit sur des backbones de réseau local (LAN) et sur des réseaux longue distance (WAN). Les médias optiques utilisent la lumière pour transmettre des données via des fibres en matière plastique ou en verre fin. Les signaux électriques amènent un émetteur à fibre optique à produire des signaux lumineux dans la fibre, que l'hôte récepteur convertit en signaux électriques à l'autre extrémité de la fibre. Cependant, le courant électrique ne circule pas dans les câbles à fibre optique, car le verre utilisé dans ce type de câble est un excellent isolant électrique.

La connectivité physique permet de partager des imprimantes, des serveurs ou des logiciels et d'accroître ainsi la productivité des utilisateurs. Dans les systèmes réseau traditionnels, les stations de travail ne peuvent être déplacées que dans les limites du média et du bureau.

L'introduction de la technologie sans fil supprime ces contraintes et confère aux réseaux informatiques une réelle portabilité. Si la technologie sans fil n'offre pas encore les transferts haut débit, la sécurité ou la fiabilité du temps de fonctionnement des réseaux câblés, son adaptabilité compense largement ces inconvénients.

Lors de l'installation ou de la mise à niveau d'un réseau, les administrateurs envisagent souvent d'utiliser la technologie sans fil, car il suffit de quelques minutes pour mettre en service les stations de travail d'un réseau sans fil simple. Une connexion câblée, un routeur, un câble ou un modem DSL assure la connectivité à Internet et un point d'accès sans fil sert de concentrateur aux nœuds sans fil. Dans un environnement résidentiel ou de petits bureaux, ces équipements peuvent être combinés en une seule unité.

Ce module porte sur certains des objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811.

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Description et installation du matériel et du logiciel requis pour pouvoir communiquer via un réseau	• Définition et description de la structure des réseaux informatiques et des technologies associées • Description du matériel et des logiciels requis pour pouvoir communiquer via un réseau • Description des propriétés et des normes physiques, électriques et mécaniques s'appliquant aux médias optiques, sans fil et de cuivre utilisés dans les réseaux • Description des
		topologies et des problèmes physiques liés au câblage des LAN les plus courants

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
3.1	Médias de cuivre
3.2	Médias optiques
3.2	Médias sans fil

- Décrire les propriétés électriques d'une matière
- Définir la tension, la résistance, l'impédance, le courant et les circuits
- Décrire les caractéristiques et les performances des différents types de câbles
- Décrire un câble coaxial ainsi que ses avantages et inconvénients par rapport aux autres types de câbles
- Décrire un câble à paires torsadées blindées et son usage
- Décrire un câble à paires torsadées non blindées et son usage
- Décrire les caractéristiques et la fonction des câbles droits, croisés et console
- Expliquer les principes des câbles à fibre optique
- Décrire la façon dont les câbles à fibre optique transportent les signaux lumineux sur de longues distances
- Décrire la fibre monomode et la fibre multimode
- Décrire le mode d'installation de la fibre optique

- Décrire le type des connecteurs et équipements utilisés avec des câbles à fibre optique
- Expliquer comment vérifier le bon fonctionnement d'un câble à fibre optique
- Identifier les problèmes de sécurité liés à la fibre optique

3.1 Médias de cuivre

3.1.1 Atomes et électrons

Cette section traite des médias de cuivre utilisés dans les réseaux. Comme toute matière est composée d'atomes, cette page commence par expliquer en détail les atomes et les électrons.

Toute matière est composée d'atomes. Le tableau périodique des éléments répertorie tous les atomes connus et leurs propriétés. Un atome est composé des trois particules suivantes:

- **Électron** – Particule de charge négative gravitant autour du noyau
- **Proton** – Particule de charge positive
- **Neutron** – Particule neutre sans charge

Les protons et les neutrons se regroupent pour former un noyau.

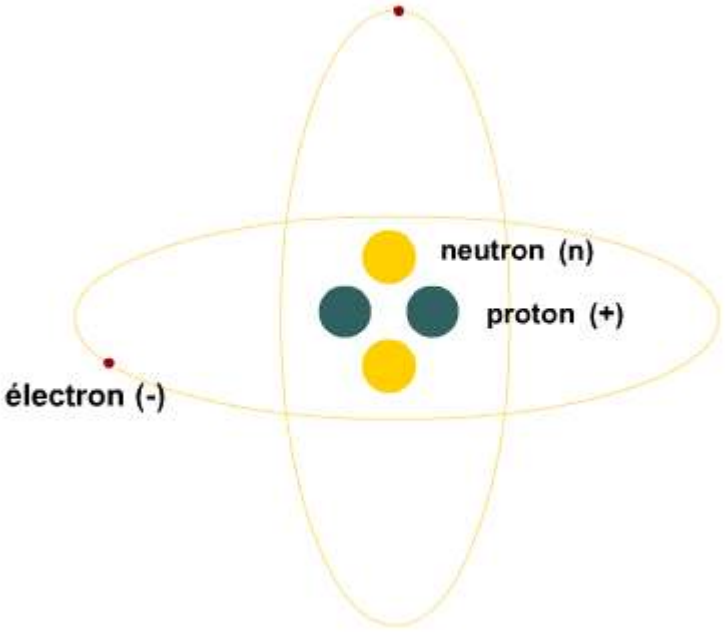
Pour mieux comprendre les propriétés électriques des différents éléments, recherchez l'hélium (He) dans le tableau périodique. 1

1 H																	2 He
3 Li	4 Be											5 B	6 C	7 N	8 O	9 F	10 Ne
11 Na	12 Mg											13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
55 Cs	56 Ba	71 Lu	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
87 Fr	88 Ra	103 Lr	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Uuu	112 Uub	113 Uut	114 Uuq	115 Uup	116 Uuh	117 Uus	118 Uuo

57 La	58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb
89 Ac	90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No

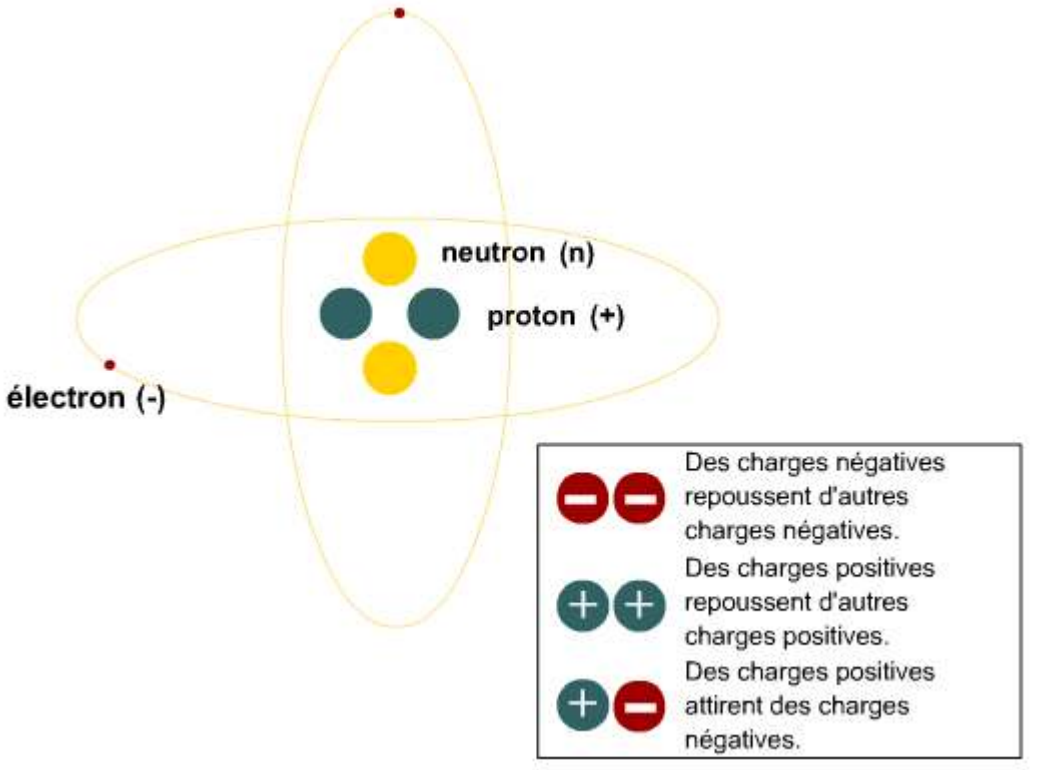
Son nombre atomique est 2, ce qui signifie qu'il est composé de deux protons et de deux électrons. Son poids atomique est 4. Si vous soustrayez de son poids son nombre atomique 2, vous obtenez le nombre de neutrons contenus dans l'hélium, soit deux neutrons.

Le physicien danois Niels Bohr a élaboré un modèle simplifié pour représenter un atome. 2



La figure suivante illustre un atome d'hélium. Si les protons et les neutrons de cet atome avaient la taille d'un ballon de football, les électrons seraient les seuls éléments plus petits que le ballon au milieu du terrain de football. Ils auraient la taille de cerises et graviteraient autour du stade près des sièges les plus éloignés du terrain. Le volume total de cet atome correspondrait à peu près à la taille du terrain et le noyau aurait la taille du ballon.

Selon la loi de Coulomb sur la force électrique, si des particules de charges opposées sont attirées l'une vers l'autre, des particules de charges identiques génèrent une force dite répulsive. Que les charges soient opposées ou identiques, la force augmente à mesure que les particules se rapprochent l'une de l'autre. La force est inversement proportionnelle au carré de la distance qui les sépare. Lorsque des particules sont très proches, la force nucléaire supplante la force électrique répulsive et préserve ainsi le noyau. C'est pourquoi le noyau ne se désintègre pas. 3


neutron (n)
proton (+)
électron (-)
Des charges négatives repoussent d'autres charges négatives.
Des charges positives repoussent d'autres charges positives.
Des charges positives attirent des charges négatives.

Examinez le modèle de l'atome d'hélium de Bohr. Si la loi de Coulomb est exacte et que le modèle de Bohr décrit les atomes d'hélium comme étant stables, d'autres lois naturelles doivent intervenir. Revoyez ces deux théories pour déterminer dans quelle mesure elles s'opposent.

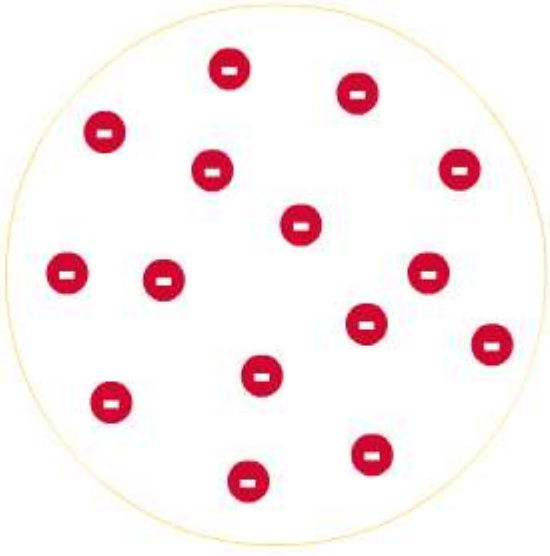
- **Loi de Coulomb** – Les charges opposées s'attirent et les charges identiques se repoussent.
- **Modèle de Bohr** – Les protons comprennent des charges positives, et les électrons des charges négatives. Le noyau contient plusieurs protons.

Les électrons restent en orbite, même si les protons attirent les électrons. Ils disposent juste de la rapidité nécessaire pour rester en orbite et ne pas être entraînés dans le noyau, à l'instar de la lune tournant autour de la terre.

Les protons restent solidaires en raison de la force nucléaire associée aux neutrons. Cette force extrêmement puissante agit comme une colle pour assurer la cohésion du noyau.

Les électrons sont liés à leur orbite autour du noyau par une force plus faible que la force nucléaire. Les électrons de certains atomes, comme les métaux, peuvent se libérer et se mettre à circuler. Cet ensemble d'électrons qui se libère facilement des atomes forme l'électricité. L'électricité résulte donc de la libre circulation des électrons.

Les électrons libérés qui ne se déplacent pas et comportent une charge négative forment l'électricité statique. 4



Des électrons proches les uns des autres ne se déplacent pas, car les champs électriques repoussant les électrons s'équilibrent. Il en résulte une force électrique nette égale à zéro.

Si ces électrons statiques entrent en contact avec un conducteur, ils génèrent une décharge électrostatique. Les conducteurs sont traités dans la suite de ce module.

Si les décharges électrostatiques sont généralement inoffensives pour les êtres humains, elles peuvent endommager gravement les équipements électroniques sensibles, tels que les puces d'un ordinateur et, le cas échéant, les données qu'il contient. Les circuits logiques des puces d'un ordinateur sont extrêmement sensibles aux décharges électrostatiques. Les étudiants devront prendre les précautions nécessaires avant d'intervenir à l'intérieur des ordinateurs, des routeurs et des équipements similaires.

Les atomes, ou groupes d'atomes (appelés molécules), constituent des matériaux. Les matériaux sont classés en trois groupes, selon la résistance qu'ils offrent aux électrons libres.

La façon dont les isolants, les conducteurs et les semi-conducteurs interagissent et contrôlent le flux d'électrons constitue la base de tout équipement électronique.

Cette activité de TP permet de revoir comment manipuler correctement un multimètre.

La page suivante décrit la tension électrique.

Activité de TP

Exercice: Utilisation et manipulation d'un multimètre en toute sécurité

Au cours de ce TP, l'étudiant va apprendre à utiliser et à manipuler correctement un multimètre.

3.1 Médias de cuivre

3.1.2 Tension

La tension électrique est parfois appelée force électromotrice.
La tension est représentée par la lettre V et, parfois, par l'abréviation FEM signifiant force électromotrice.
L'unité de mesure de la tension est le volt (V).

Cette page décrit la tension électrique.

La tension électrique est parfois appelée force électromotrice. Il s'agit de la force électrique, ou pression, qui s'exerce lors de la séparation des électrons et des protons. Il se produit ainsi une force d'attraction entre des charges opposées et une force de répulsion entre des charges identiques. Ce processus se produit dans une batterie où une action chimique libère les électrons du pôle négatif de la batterie, qui se dirigent alors vers le pôle opposé (positif) de la batterie, via un circuit externe. Ils ne circulent pas à l'intérieur de la batterie. Gardez toujours présent à l'esprit que le flux d'électricité est en réalité un flux d'électrons. La tension électrique peut également être produite par trois autres procédés : par friction (électricité statique), par magnétisme (générateur électrique) et par la lumière (photopile).

La tension est représentée par la lettre «V» et, parfois, par les lettres «FEM» signifiant force électromotrice. L'unité de mesure de la tension est le volt (V). 1 Un volt est défini comme le travail nécessaire, par unité de charge, pour séparer les charges.

Au cours de ce TP, les étudiants vont mesurer la tension.

La page suivante décrit la résistance et l'impédance.

Activité de TP

Exercice: Mesure de la tension

Au cours de ce TP, les étudiants vont démontrer leur aptitude à mesurer la tension en toute sécurité avec un multimètre.

3.1 Médias de cuivre

3.1.3 Résistance et impédance

Cette page explique les concepts de résistance et d'impédance.

La résistance au mouvement des électrons varie en fonction des matériaux à travers lesquels circule le courant. Les matériaux qui offrent très peu de résistance, voire aucune, sont appelés conducteurs. Ceux qui freinent la circulation du courant ou s'y opposent fortement sont appelés isolants. Le degré de résistance dépend de la composition chimique des matériaux.

Tous les matériaux qui conduisent l'électricité sont dotés d'une mesure de résistance au flux d'électrons qui les traverse. La capacitance et l'inductance sont d'autres effets liés au flux d'électrons, dont sont dotés ces matériaux. L'impédance, qui inclut la résistance, la capacitance et l'inductance, est similaire au concept de résistance.

L'atténuation est également une mesure importante dans le domaine des réseaux. Elle est liée à la résistance au flux d'électrons et explique pourquoi un signal se dégrade lorsqu'il se déplace dans un conduit.

La lettre «R» représente la résistance et l'unité de mesure de la résistance est l'ohm (**Ω**). Ce symbole correspond à la lettre grecque oméga.

Les isolants électriques sont les matériaux les plus résistants au flux d'électrons qui les traverse. La matière plastique, le verre, l'air, le bois sec, le papier, le caoutchouc et l'hélium sont des exemples d'isolants électriques. Leur structure chimique est très stable et les électrons sont étroitement liés à l'intérieur des atomes.

En revanche, les conducteurs électriques facilitent la circulation des électrons. Les électrons les plus éloignés du noyau ne sont pas étroitement liés à celui-ci et peuvent se libérer facilement. À température ambiante, ces matériaux comptent un grand nombre d'électrons libres qui favorisent la conduction. L'ajout d'une tension électrique entraîne le déplacement des électrons, ce qui produit un courant.

Le tableau périodique classe en colonnes certains groupes d'atomes. Les atomes de chaque colonne appartiennent à une famille chimique donnée. Même si leur nombre de protons, de neutrons et d'électrons est différent, les électrons les plus éloignés du noyau ont des orbites et des interactions semblables à celles des autres atomes et molécules. Les meilleurs conducteurs sont les métaux tels que le cuivre (Cu), l'argent (Ag) et l'or (Au). Les électrons de ces métaux se libèrent facilement. La brasure tendre (mélange de plomb (Pb) et d'étain (Sn)) et l'eau ionisée sont d'autres exemples de conducteurs. Un ion est un atome dont le nombre d'électrons est différent du nombre de protons dans le noyau. Le corps humain est composé d'environ 70 % d'eau ionisée, ce qui signifie qu'il est, lui aussi, un conducteur.

Les semi-conducteurs sont des matériaux dans lesquels la quantité d'électricité qui circule peut être contrôlée de manière précise. Ces matériaux sont regroupés dans une même colonne du tableau périodique. Cette catégorie de matériaux comprend le carbone (C), le germanium (Ge) et un alliage, l'arséniure de gallium (AsGa). Le silicium (Si) est le semi-conducteur le plus important, car il constitue le meilleur circuit électronique microscopique.

Le silicium est très répandu ; il est présent dans le sable, le verre et un grand nombre de roches. La région s'étendant autour de San Jose, en Californie, est appelée Silicon Valley parce que l'industrie informatique à base de puces de silicium a démarré à cet endroit. 1

Isolants	Conducteurs	Semi-conducteurs
Les électrons circulent difficilement	Les électrons circulent facilement	Le flux d'électrons peut être contrôlé de manière précise
Matière plastique Caoutchouc Air Papier Bois sec Verre	Cuivre (Cu) Argent (Ag) Or (Au) Soudure Eau ionisée Corps humain	Carbone (C) Germanium (Ge) Arséniure de gallium (AsGa) Silicium (Si)

Au cours de l'activité de TP, les étudiants vont apprendre à mesurer la résistance et la continuité.

Au cours de l'activité de média interactive, ils vont apprendre à identifier les caractéristiques de résistance et d'impédance de différents matériaux.

La page suivante décrit le courant électrique.

Activité de TP

Exercice: Mesure de la résistance

Au cours de ce TP, les étudiants vont démontrer leur aptitude à mesurer la résistance et la continuité avec un multimètre.

Activité de média interactive

Glisser-Positionner: Isolants, conducteurs et semi-conducteurs

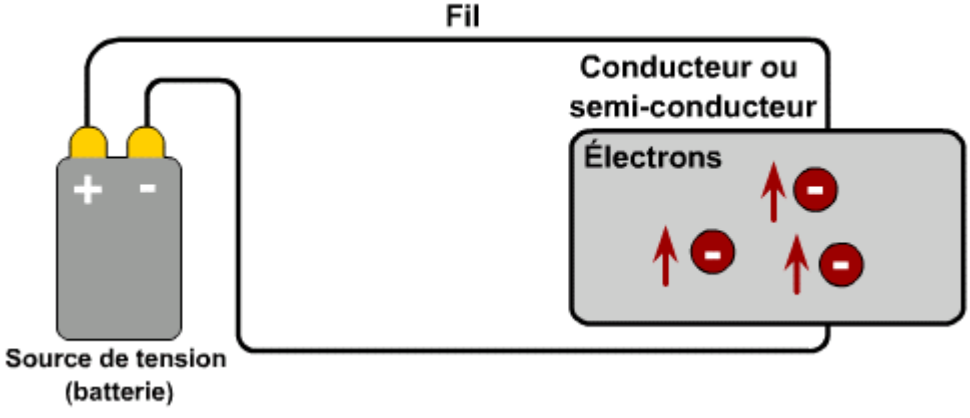
À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques de résistance et d'impédance de différents matériaux.

3.1 Médias de cuivre

3.1.4 Courant

Cette page décrit en détail le courant électrique.

Le courant électrique est le flux de charges créé par le déplacement des électrons. Dans les circuits électriques, le courant est produit par un flux d'électrons libres. Lorsqu'une tension est appliquée et que le courant dispose d'une voie pour circuler, les électrons se déplacent depuis la borne négative (qui les repousse) vers la borne positive (qui les attire). 1



Fenêtre contextuelle (pop up)

Lorsqu'une tension, par exemple une batterie, est appliquée à un conducteur ou à un semi-conducteur, les électrons se déplacent vers la borne positive de la batterie.

Ce flux est un exemple de courant électrique. Le chemin réel des électrons est plus complexe que cela.

Le courant électrique est représenté par le symbole I et mesuré en unités appelées ampères. L'abréviation de l'ampère est A.

La borne négative repousse les électrons, et la borne positive les attire. La lettre «I» représente le courant. L'unité de mesure du courant est l'ampère (A). Un ampère est le nombre de charges par seconde passant par un point dans un circuit.

Le courant correspond au nombre d'électrons qui circulent, c'est-à-dire au volume du trafic d'électrons, et la tension correspond à la vitesse du trafic. La combinaison volts-ampères produit des watts. La puissance des appareils électriques tels que les ampoules, les moteurs et l'alimentation des ordinateurs est évaluée en watts. Les watts indiquent la puissance consommée ou produite par ce type d'appareil.

Il s'agit de l'intensité du courant, ou ampérage, d'un circuit électrique réellement actif. Par exemple, l'électricité statique peut engendrer un choc électrique mais pas de blessure permanente, car elle offre un faible ampérage malgré une tension élevée pouvant franchir jusqu'à 2,5 cm. Le démarreur d'une automobile opère à une tension relativement faible (12 volts), mais requiert un ampérage élevé pour générer suffisamment d'énergie et faire tourner le moteur. La combinaison d'une tension et d'un ampérage élevées, comme la foudre, peut provoquer de graves dommages ou blessures.

La page suivante décrit les circuits électriques.

3.1 Médias de cuivre

3.1.5 Circuits

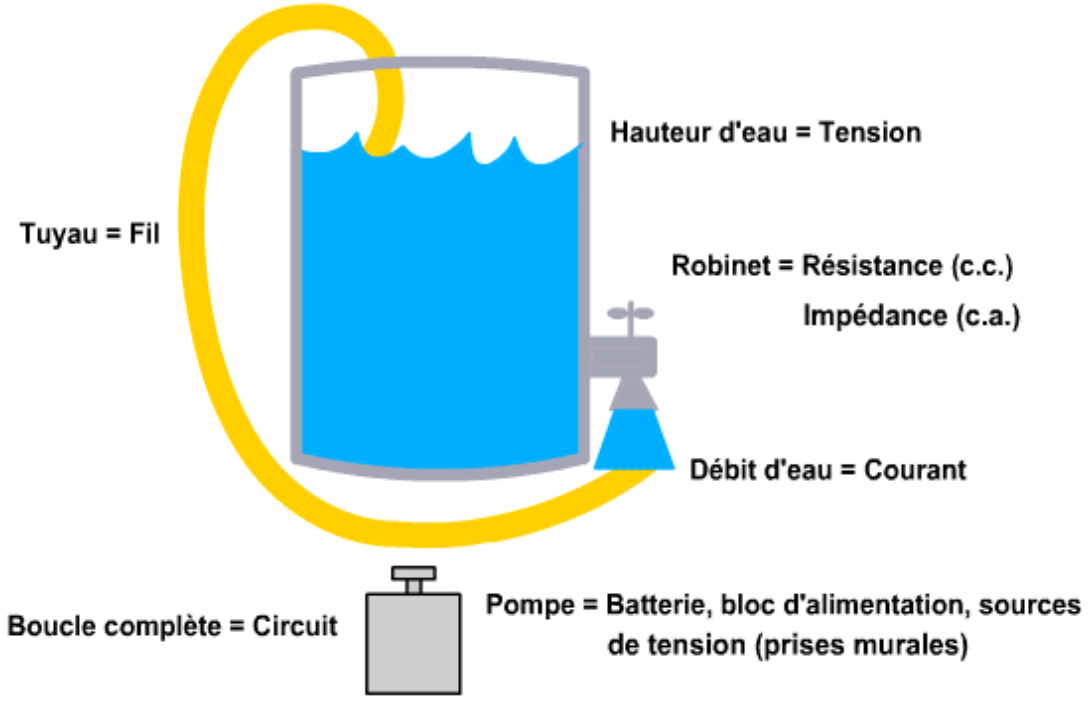
Cette page décrit les circuits électriques.

Le courant circule dans des boucles fermées appelées circuits. Ces circuits doivent être composés de matériaux conducteurs et posséder une source de tension. Si la tension permet au courant de circuler, la résistance et l'impédance s'y opposent. Le courant est composé d'électrons qui se déplacent depuis une borne négative vers une borne positive. Toutes ces données connues facilitent le contrôle du flux de courant.

L'électricité se dirige naturellement vers la terre si elle dispose d'une voie. Le courant emprunte également la voie qui offre la résistance la plus faible. C'est ainsi qu'il peut traverser le corps humain s'il rencontre peu de résistance. Lorsque vous utilisez un appareil électrique muni d'une fiche à trois broches, l'une des broches sert de contact de mise à la terre. Cette broche conduit les électrons jusqu'à la terre. La résistance du corps humain serait supérieure à celle de la terre.

En général, la terre correspond au niveau de référence 0 volt dans les mesures électriques. Comme la tension résulte de la séparation de particules chargées, elle doit être mesurée entre deux points.

Une analogie avec l'eau permet de mieux comprendre le concept de l'électricité. Plus l'eau tombe de haut et plus la pression est grande, plus le débit est fort. Le débit de l'eau dépend également de la taille de l'espace à travers lequel elle coule. De même, plus la tension et la pression électrique sont élevées, plus le courant produit est important. Le courant électrique rencontre alors une résistance, à la façon d'un robinet qui réduit le débit de l'eau. S'il s'agit d'un circuit de courant alternatif, la quantité de courant dépendra de l'impédance du matériau. S'il s'agit d'un circuit de courant continu, la quantité de courant dépendra de la résistance du matériau. Une pompe agit comme une batterie. Elle fournit la pression nécessaire pour assurer la circulation de l’eau. 1

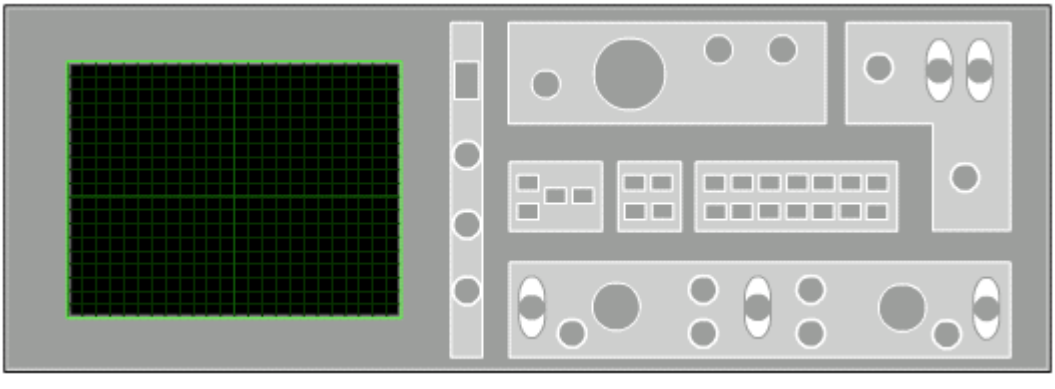

Hauteur d'eau = Tension
Tuyau = Fil
Robinet = Résistance (c.c.)
Impédance (c.a.)
Débit d'eau = Courant
Boucle complète = Circuit
Pompe = Batterie, bloc d'alimentation, sources de tension (prises murales)

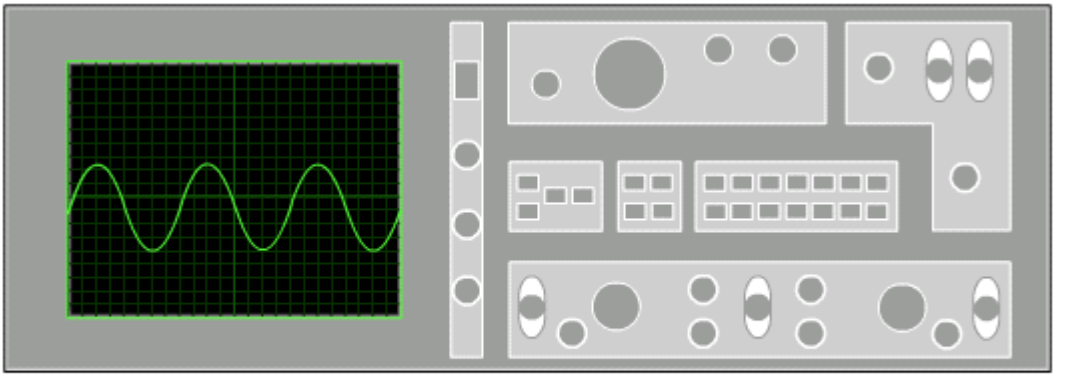
La relation entre la tension, la résistance et le courant est la tension (V) qui est égale au courant (I) multiplié par la résistance (R). Autrement dit, V=I*R. Cette formule fondamentale découverte par le physicien Ohm, est appelée loi d'Ohm.

Le courant peut circuler de façon alternative et de façon continue. Les tensions alternatives changent de polarité ou de direction en fonction du temps. Le courant alternatif (c.a.) circule dans un sens, puis dans l'autre, et répète le processus. La tension alternative est positive à une borne, et négative à l'autre, puis elle inverse sa polarité de sorte que la borne positive devient négative et la borne négative, positive. Ce processus se répète en permanence.

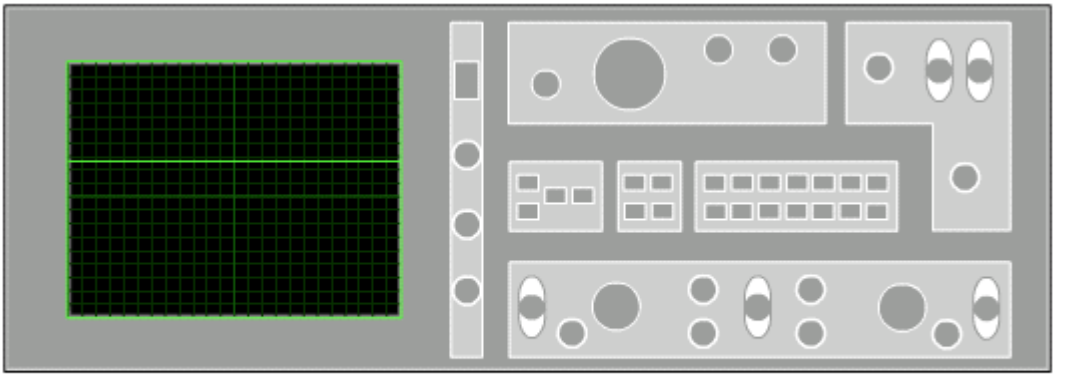
En revanche, le courant continu (c.c.) circule toujours dans la même direction et la tension continue a toujours la même polarité. Une borne est toujours positive et l'autre, toujours négative. Elles ne sont jamais inversées.

Un oscilloscope est un appareil électronique qui permet de mesurer les signaux électriques par rapport au temps. Il trace les ondes et les impulsions électriques, ainsi que les caractéristiques des signaux électriques. L'axe des x représente le temps, et l'axe des y la tension. 2





AC

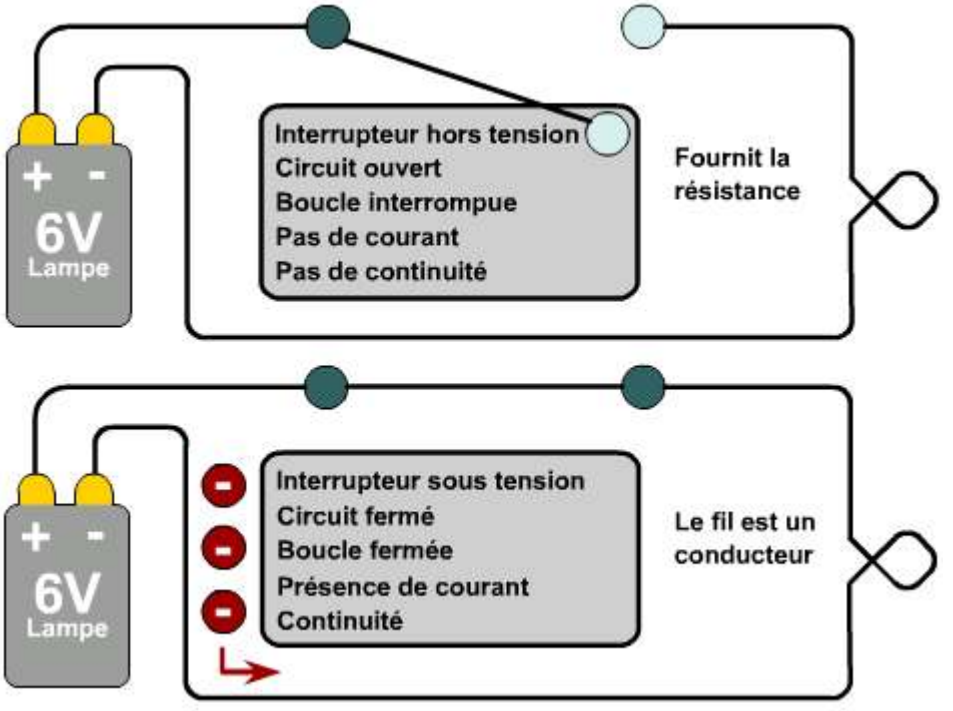


DC

L'axe des y comprend généralement deux entrées de tension afin qu'il soit possible d'observer et de mesurer deux ondes simultanément.

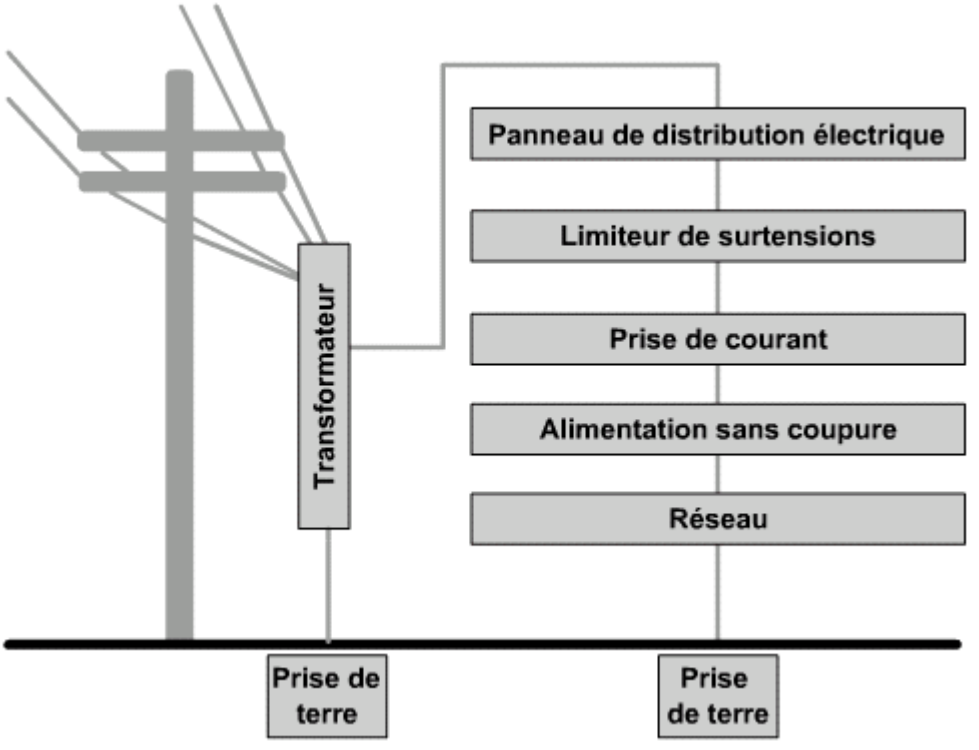
Les lignes d'alimentation transportent l'électricité sous forme de courant alternatif afin de l'acheminer efficacement sur de longues distances. Le courant continu circule sur une courte distance. C'est pourquoi, il alimente, par exemple, les piles de lampe de poche, les batteries de véhicule et les puces de la carte mère d'un ordinateur.

Les électrons circulent dans des circuits fermés, ou boucles complètes. La figure 3



représente un circuit simple. Les processus chimiques d'une batterie génèrent des charges qui produisent une tension, ou pression électrique, entraînant la circulation des électrons à travers divers équipements. Les lignes représentent un conducteur, généralement un fil de cuivre. Un interrupteur est comparable aux deux extrémités d'un fil qui peuvent être ouvertes ou rompues afin d'empêcher la circulation des électrons. Lorsque les deux extrémités sont fermées, fixées ou court-circuitées, les électrons peuvent circuler librement. Enfin, une ampoule offre une résistance au flux d'électrons, ce qui entraîne un dégagement d'énergie de la part des électrons sous forme de lumière. Les circuits des réseaux sont beaucoup plus complexes que ce type de circuit.

Dans tout circuit électrique à courant alternatif ou continu, le flux d'électrons se déplace toujours d'une source chargée négativement vers une source chargée positivement. Toutefois, un circuit complet est nécessaire pour générer un flux contrôlé d'électrons. La figure 4



représente une partie d'un circuit électrique qui alimente une habitation ou un bureau.

L'activité de TP est consacrée aux propriétés fondamentales des circuits en série.

La page suivante traite des spécifications des câbles.

Activité de TP

Exercice: Circuits en série

Au cours de ce TP, l'étudiant va fabriquer des circuits en série et étudier leurs propriétés fondamentales.

3.1 Médias de cuivre

3.1.6 Spécifications des câbles

Cette page décrit les spécifications des câbles et les attentes.

Les spécifications des câbles et les attentes étant différentes, il est important de tenir compte des considérations suivantes liées aux performances:

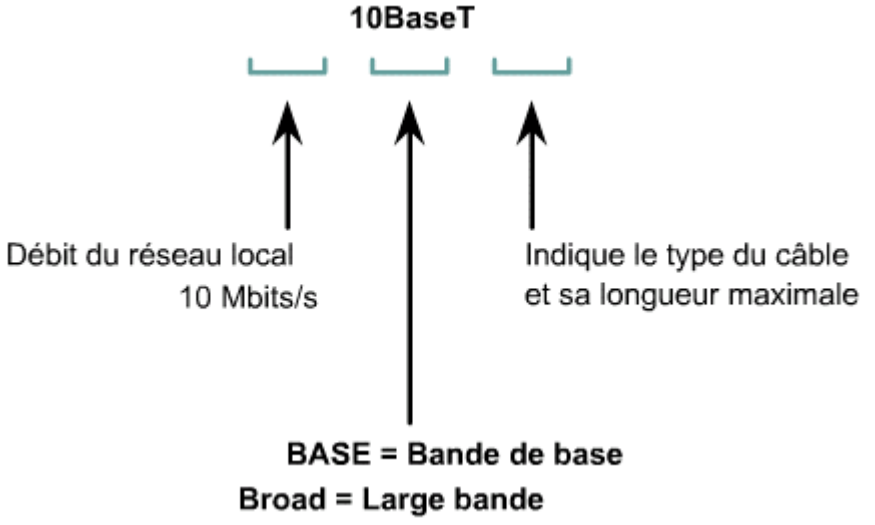
- À quelles vitesses la transmission de données peut-elle être réalisée ? La vitesse de transmission des bits dans un câble est extrêmement importante. Le type de conduit utilisé influence la vitesse de transmission.
- Les transmissions doivent-elles être numériques ou analogiques ? La transmission numérique ou à bande de base nécessite des types de câble différents de ceux utilisés pour la transmission analogique ou à large bande.
- Quelle distance un signal peut-il parcourir avant que l'atténuation n'affecte la transmission ? Si le signal est dégradé, les équipements réseau ne peuvent ni le recevoir ni l'interpréter. La distance

parcourue par le signal dans le câble influe sur l'atténuation du signal. La dégradation est directement liée à la distance parcourue par le signal et au type de câble utilisé.

Les spécifications Ethernet suivantes se rapportent au type de câble:

- 10BaseT
- 10Base5
- 10Base2

10BaseT indique une vitesse de transmission de 10 Mbits/s. 1



La transmission est du type à bande de base ou interprétée numériquement. La lettre T indique une paire torsadée.

10Base5 indique une vitesse de transmission de 10 Mbits/s. La transmission est du type à bande de base ou interprétée numériquement. Le chiffre 5 indique qu'un signal peut parcourir environ 500 mètres avant que l'atténuation ne puisse empêcher le récepteur d'interpréter le signal. La spécification 10Base5 est souvent appelée ThickNet. Ethernet à câble épais (Thicknet) est un type de réseau alors que 10BASE5 est la norme Ethernet utilisée dans ce réseau.

10Base2 indique une vitesse de transmission de 10 Mbits/s. La transmission est du type à bande de base ou interprétée numériquement. Le chiffre 2 indique qu'une longueur de segment maximale de 200 mètres peut être parcourue avant que l'atténuation ne puisse empêcher le récepteur d'interpréter correctement le signal reçu. La longueur de segment maximale est en fait de 185 mètres. La spécification 10Base2 est souvent appelée ThinNet. Ethernet à câble fin (Thinnet) est un type de réseau alors que 10BASE2 est la norme Ethernet utilisée dans ce réseau.

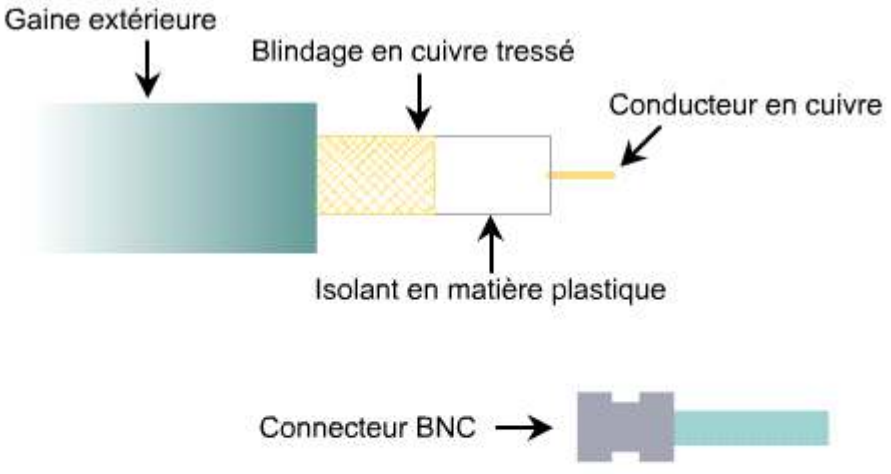
La page suivante décrit le câble coaxial.

3.1 Médias de cuivre

3.1.7 Câble coaxial

Cette page décrit en détail le câble coaxial.

Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible. 1



- Vitesse et débit : 10 à 100 Mbits/s
- Coût : Économique
- Taille du connecteur et du média : Moyenne
- Longueur de câble maximale : 500 m

Le conducteur central peut également être un câble d'aluminium recouvert de fer-blanc dans les installations bon marché. Sur ce matériau isolant, un revêtement de cuivre tressé ou un film métallique constitue le second fil du circuit et protège le conducteur intérieur. Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes. La gaine du câble enveloppe ce blindage.

Un câble coaxial présente plusieurs avantages pour les réseaux locaux. Il peut couvrir des distances plus longues que les câbles à paires torsadées blindées (STP), à paires torsadées non blindées (UTP) ou ScTP *(screened twisted pair)*, sans nécessiter de répéteurs. Les répéteurs régénèrent les signaux du réseau pour qu'ils puissent parcourir de plus grandes distances. Le câble coaxial est moins onéreux que le câble à fibre optique et sa technologie est bien connue. Il est utilisé depuis de nombreuses années dans divers types de communication de données, notamment dans les réseaux de télévision câblée.

La taille du câble est un paramètre important. Plus il est épais, plus il est difficile à manipuler. N'oubliez pas qu'il faut tirer les câbles dans des conduits étroits. La taille des câbles coaxiaux est variable. Le diamètre le plus large était recommandé pour le câblage de backbone Ethernet, car il assurait une distance de transmission plus longue et offrait des caractéristiques de protection supérieures contre le bruit. Ce type de câble coaxial est souvent appelé câble Ethernet épais. Toutefois, ce type de câble peut s'avérer trop rigide dans certaines installations. En règle générale, plus un média réseau est difficile à installer, plus l'installation est onéreuse. L'installation d'un câble coaxial est plus onéreuse que celle d'un câble à paires torsadées. Les câbles Ethernet épais ne sont presque plus utilisés ; ils sont désormais réservés à des installations spécifiques.

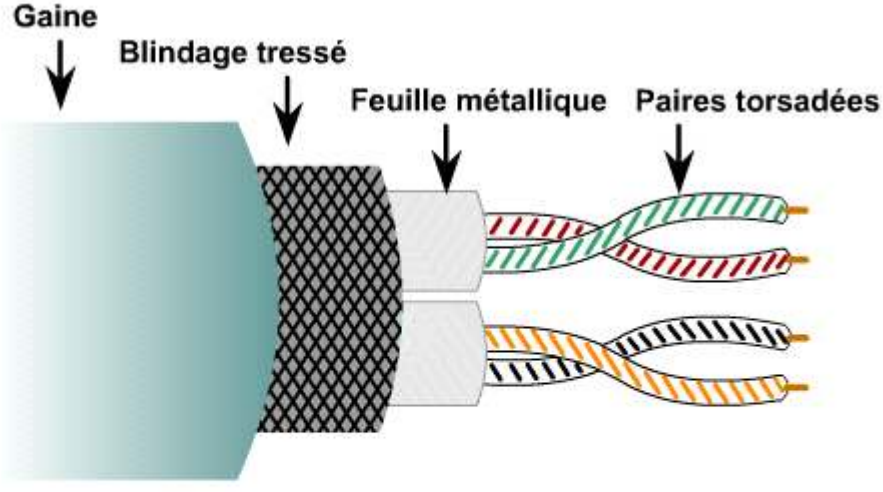
Le câble coaxial Ethernet fin d'un diamètre externe de 0,35 cm maximum était auparavant utilisé dans les réseaux Ethernet. En raison de sa souplesse, il s'avérait particulièrement utile dans les installations sinueuses comportant des angles et des tournants. Comme il était facile à installer, il était également plus économique. Comme la torsade de cuivre ou de métal d'un câble coaxial constitue la moitié du circuit électrique, il est important de disposer d'une connexion électrique robuste aux deux extrémités du câble pour assurer une mise à la terre correcte. Une connexion blindée défectueuse est une des causes les plus importantes des problèmes de connexion dans l'installation d'un câble coaxial. Les problèmes de connexion se traduisent souvent par du bruit électrique qui perturbe la transmission des signaux. C'est pourquoi, le câble Ethernet fin n'est plus utilisé, ni pris en charge par les dernières normes de réseau Ethernet 100 Mbits/s et supérieures.

La page suivante décrit le câble à paires torsadées blindées (STP).

3.1 Médias de cuivre
3.1.8 Câble à paires torsadées blindées (STP)

Cette page décrit en détail le câble à paires torsadées blindées.

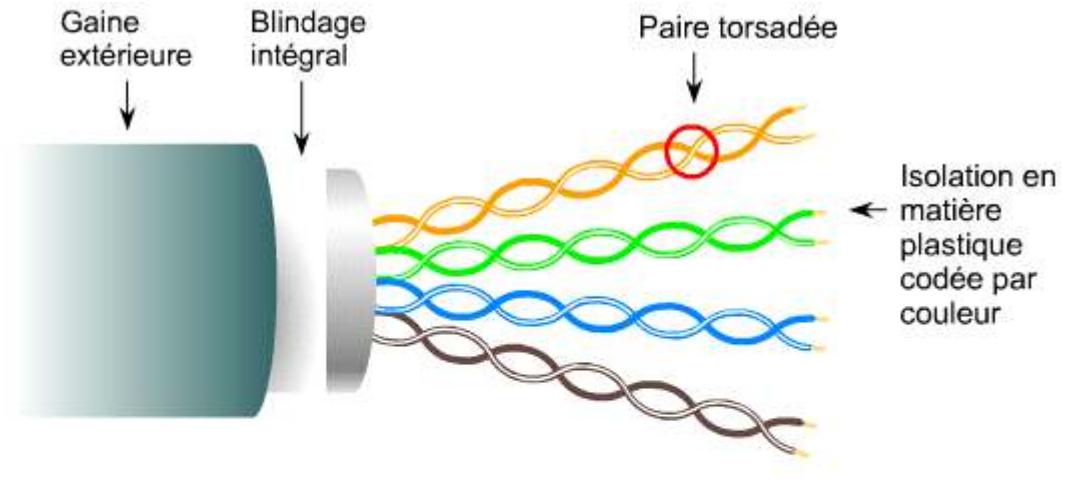
Le câble à paires torsadées blindées allie les techniques de blindage, d'annulation et de torsion des fils. 1



- Vitesse et débit : 0 à 100 Mbits/s
- Coût : Modéré
- Taille du connecteur et du média : Moyenne à grande
- Longueur de câble maximale : 100 m

Chaque paire de fils est enveloppée dans une feuille métallique et les deux paires sont enveloppées ensemble dans un revêtement tressé ou un film métallique. Il s'agit généralement d'un câble de 150 ohms. Comme l'indiquent les instructions d'installation de réseau Token Ring, les paires torsadées blindées réduisent le bruit électrique à l'intérieur du câble (couplage paire à paire ou diaphonie), ainsi qu'à l'extérieur du câble (interférences électromagnétiques et radio). Le câble à paires torsadées blindées (STP) présente plusieurs avantages et inconvénients communs au câble à paires torsadées non blindées (UTP). Le câble STP assure une protection plus efficace contre toutes les interférences externes, mais il est plus onéreux et plus difficile à installer qu'un câble UTP.

Le câble ScTP *(screened twisted pair)* ou FTP *(foil screened twisted pair)* est un nouveau type de câble UTP hybride.



- Vitesse et débit : 0 à 100 Mbits/s
- Coût : Moyennement onéreux
- Taille du connecteur et du média : Moyenne à grande
- Longueur de câble maximale : 100 m

Comme le câble UTP, le câble ScTP est un câble de 100 ohms. Un grand nombre d'installateurs et de fabricants de câbles utilisent le terme STP pour désigner les câbles ScTP. Il est important de retenir que le terme STP désigne en fait un câble à quatre paires torsadées blindées et que le véritable câble STP est rarement utilisé dans les installations actuelles.

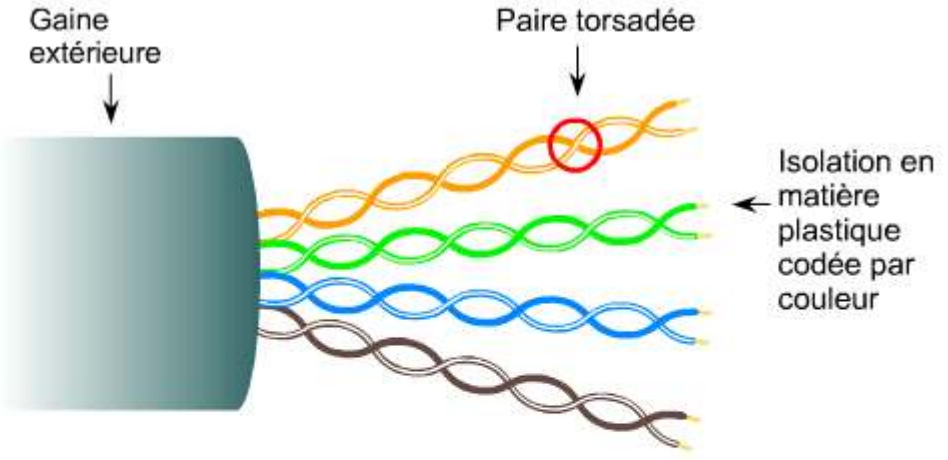
Le matériau de protection métallique des paires torsadées blindées doit être mis à la terre aux deux extrémités. Si la mise à la terre est incorrecte ou s'il existe des discontinuités sur la longueur du matériau de protection, les paires torsadées blindées risquent de provoquer des problèmes de bruit importants, car le film protecteur se comporte comme une antenne qui attire des signaux indésirables. Toutefois, cet effet fonctionne dans les deux sens : le film protecteur empêche les ondes électromagnétiques entrantes de provoquer du bruit sur les fils de données et réduit les ondes électromagnétiques sortantes susceptibles de produire du bruit dans les autres équipements. Un câble à paires torsadées blindées ne peut pas être aussi long que les autres médias réseau tels que le câble coaxial ou à fibre optique, sans que le signal soit répété. L'isolation et le blindage augmentent considérablement la taille, le poids et le coût du câble. De plus, les terminaisons sont plus difficiles à réaliser. Cependant, le câble à paires torsadées blindées est toujours utilisé, particulièrement en Europe et dans des installations où les interférences électromagnétiques et radio sont fréquentes.

La page suivante décrit le câble à paires torsadées non blindées (UTP).

3.1 Médias de cuivre

3.1.9 Câble à paires torsadées non blindées (UTP)

Cette page décrit en détail le câble à paires torsadées non blindées.

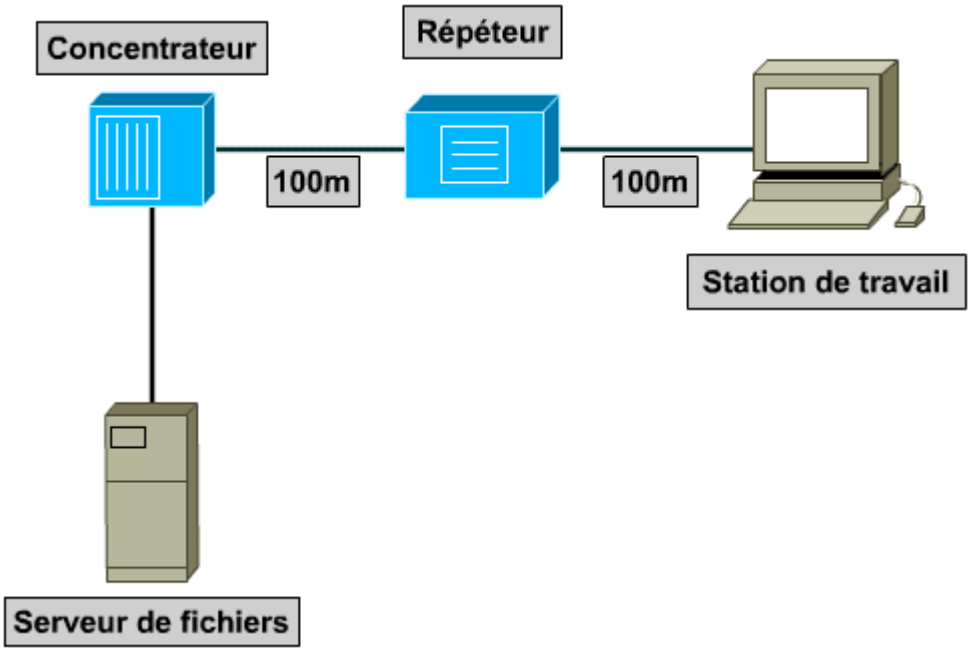


- Vitesse et débit : 10 - 100 - 1000 Mbits/s (selon la qualité/catégorie du câble)
- Coût : Le moins onéreux
- Taille du connecteur et du média : Petite
- Longueur de câble maximale : 100 m

Le câble à paires torsadées non blindées (UTP) 1 est un média constitué de quatre paires de fils, présent dans divers types de réseau. Chacun des huit fils de cuivre du câble est protégé par un matériau isolant. De plus, les paires de fils sont tressées entre elles. Ce type de câble repose uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et radio. La réduction de la diaphonie entre les paires d'un câble à paires torsadées non blindées dépend du nombre de torsades. Comme le câble STP, le câble UTP doit respecter précisément le nombre de torsades autorisées par mètre.

La norme TIA/EIA-568-B.2 comprend des spécifications liées aux performances des câbles. Elle implique la connexion de deux câbles à chaque prise, l'un pour la voix et l'autre pour les données. Le câble destiné à la voix doit être un câble à quatre paires torsadées non blindées. Le câble de catégorie 5e est le plus souvent recommandé et utilisé dans les nouvelles installations. Cependant, les experts et les instituts de sondage prévoient que les câbles de catégorie 5e seront bientôt remplacés par les câbles de catégorie 6 dans les installations de réseau. Comme les spécifications de canal et de liaison des câbles de catégorie 6 sont compatibles en amont avec les câbles de catégorie 5e, elles facilitent le remplacement des câbles de catégorie 5. Les applications qui fonctionnent avec des câbles de catégorie 5e fonctionneront avec des câbles de catégorie 6.

Le câble UTP présente de nombreux avantages. Il est facile à installer et moins onéreux que les autres types de média réseau. Son prix au mètre est inférieur à celui de tout autre type de câble de réseau local. 2



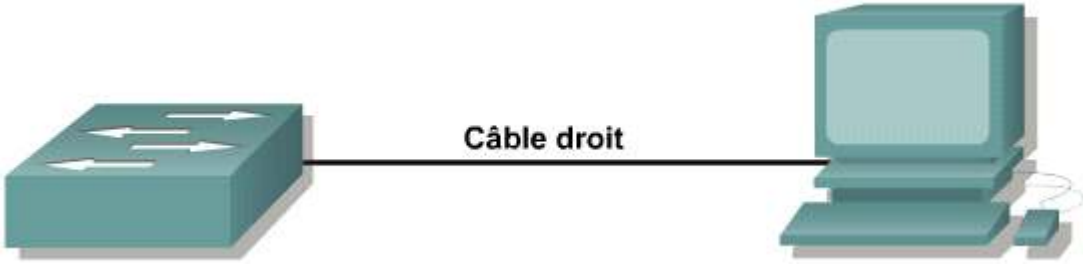
Sa taille constitue un réel avantage. Grâce à son diamètre de petite taille, il est possible de loger dans un conduit plus de câbles à paires torsadées non blindées que d'autres types de câble. Cet avantage est particulièrement important lors de l'installation d'un réseau dans un immeuble ancien. De plus, un câble UTP muni d'un connecteur RJ-45 réduit considérablement les sources de bruit potentielles, ce qui améliore la fiabilité de la connexion.

Cependant, un câble à paires torsadées non blindées présente aussi des inconvénients. Il est plus sensible au bruit électrique et aux interférences que les autres types de média réseau, et l'écart entre les amplifications du signal est plus court sur un câble UTP que sur un câble coaxial ou à fibre optique.

Auparavant, la transmission des données sur un câble à paires torsadées était plus lente que sur les autres types de câble, mais ce n'est plus vrai actuellement. Aujourd'hui, le câble à paires torsadées est considéré comme le média de cuivre le plus rapide.

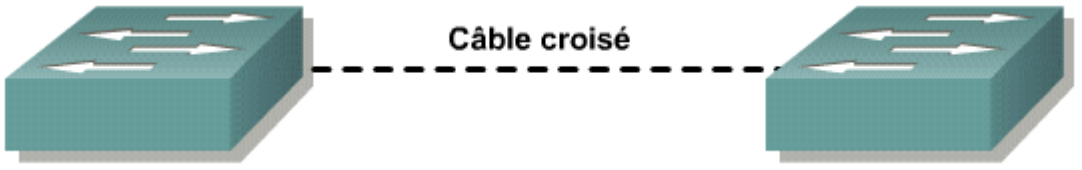
Pour que la communication s'établisse, le signal transmis par la source doit être compris par la destination, aussi bien du point de vue logiciel que physique. Le signal transmis doit être réceptionné correctement par la connexion de circuit destinée à recevoir des signaux. La broche d'envoi de données de la source doit enfin se connecter à la broche de réception de la destination. Les types de connexion câblée suivants sont utilisés entre des équipements interréseau.

La figure 3



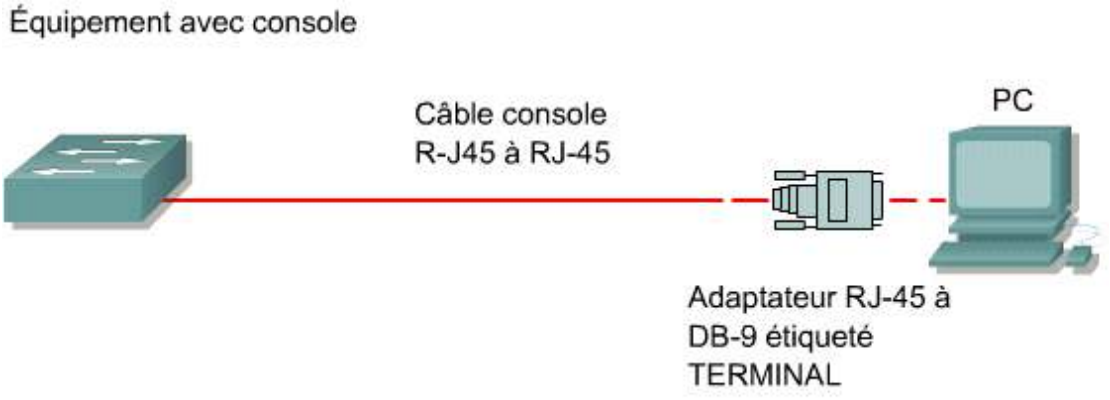
représente un commutateur LAN connecté à un ordinateur. Le câble reliant le port du commutateur au port de la carte réseau de l'ordinateur est un câble droit.

La figure 5



représente deux commutateurs connectés entre eux. Le câble reliant un port de commutateur à l'autre est un câble croisé.

Dans la figure 7



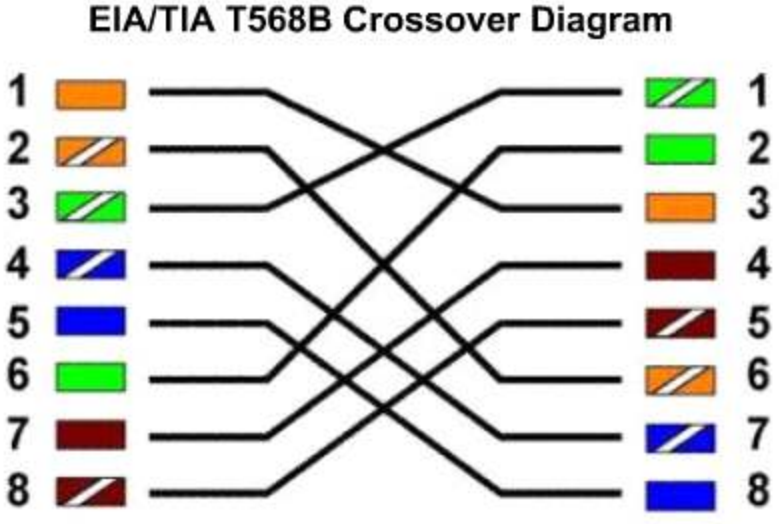
- Les PC nécessitent un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25.
- Paramètres du port COM : 9 600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et pas de contrôle de flux.
- Fournit un accès hors bande à la console.
- Le port de commutateur AUX peut être utilisé pour une console connectée par modem.

, le câble reliant l'adaptateur RJ-45 du port COM de l'ordinateur au port console du routeur ou du commutateur est un câble console ou un câble à paires inversées.

Les câbles sont définis par le type des connexions ou des configurations de broches d'une extrémité à l'autre du câble. Reportez-vous aux figures 4

Broche 1 ---------- Broche 1
Broche 2 ---------- Broche 2
Broche 3 ---------- Broche 3
Broche 4 ---------- Broche 4
Broche 5 ---------- Broche 5
Broche 6 ---------- Broche 6
Broche 7 ---------- Broche 7
Broche 8 ---------- Broche 8

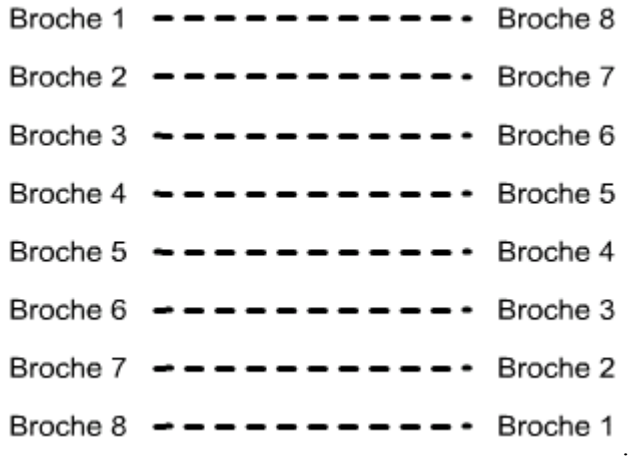
,



Seuls quatre fils (1, 2, 3 et 6) sont actifs dans un câble d'interconnexion Ethernet (10BaseT et 100BaseTX)

6

et 8



Un technicien peut comparer les deux extrémités du même câble en les plaçant l'une à côté de l'autre avant d'encastrer le câble dans un mur. Il peut observer les couleurs des deux connexions RJ-45 en les maintenant bout à bout par la pince et en dirigeant vers le haut les deux extrémités du câble. L'ordre des couleurs des fils d'un câble droit doit être identique aux deux extrémités. La couleur des fils des broches 1 et 2 d'une extrémité d'un câble croisé doit être la même que celle des fils des broches 3 et 6 de l'autre extrémité, et inversement, car les emplacements des broches de transmission et de réception sont différents. Dans un câble console ou à paires inversées, la combinaison des couleurs de gauche à droite d'une extrémité doit être exactement l'inverse de celle de l'autre extrémité.

Au cours de la première activité de TP, les étudiants concevront, fabriqueront et testeront un système de communication simple.

Au cours de la deuxième activité de TP, ils utiliseront un testeur de câble pour déterminer l'état d'un câble droit ou croisé.

Au cours de la troisième activité de TP, ils apprendront à fabriquer un câble droit, un câble console et un câble croisé.

Au cours de la dernière activité de TP, ils rechercheront les prix de différents câbles.

Cette leçon est terminée. La leçon suivante traite des médias optiques. La première page est consacrée au spectre électromagnétique.

Activité de TP

Exercice: Circuits de communication

Au cours de ce TP, les étudiants vont concevoir, fabriquer et tester un système de communication simple.

Activité de TP

Exercice: Tests de câble élémentaires au moyen du Fluke 620

Au cours de ce TP, les étudiants vont vérifier l'état d'un câble droit ou croisé à l'aide d'un testeur de câble simple.

Activité de TP

Exercice: Fabrication d'un câble droit

Au cours de ce TP, les étudiants vont fabriquer et tester un câble de raccordement Ethernet UTP de catégorie 5 ou 5e.

Activité de TP

Exercice: Fabrication d'un câble console (à paires inversées)

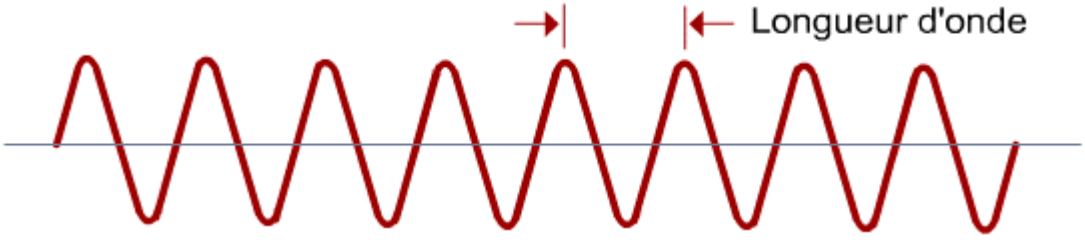
Au cours de ce TP, les étudiants vont fabriquer un câble console (à paires inversées) UTP de catégorie 5 ou 5e, puis ils vérifieront sa continuité et la configuration des broches.

.2 Médias optiques

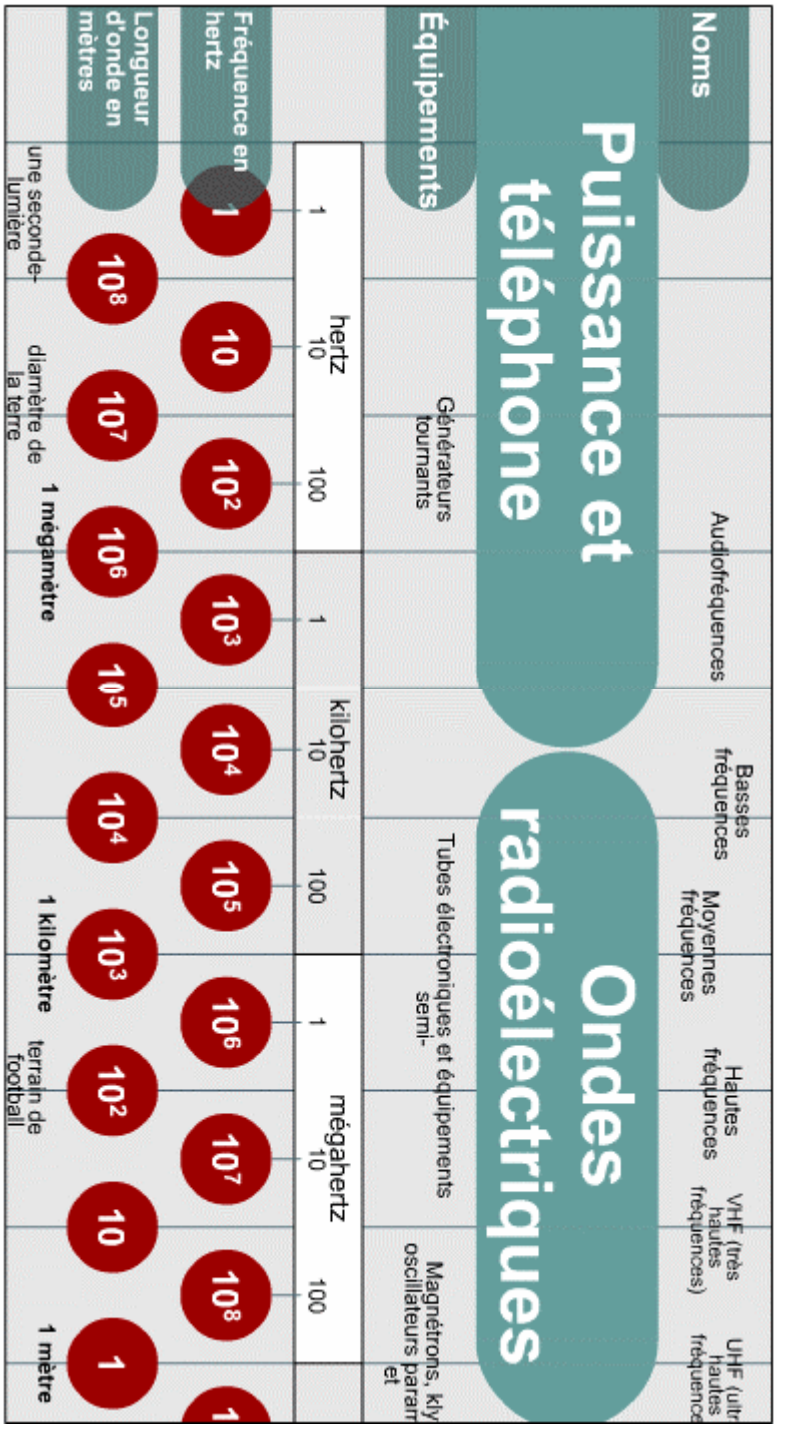
3.2.1 Spectre électromagnétique

Cette page présente le spectre électromagnétique.

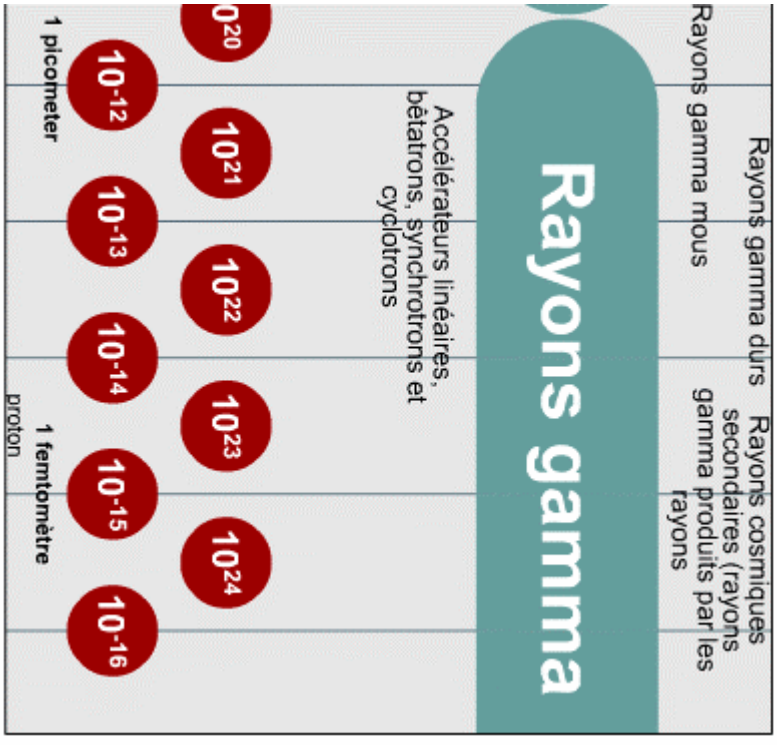
La lumière utilisée dans les réseaux à fibre optique est un type d'énergie électromagnétique. Lorsqu'une charge électrique va et vient ou accélère, elle produit de l'énergie électromagnétique. Cette énergie se déplace sous la forme d'ondes dans le vide, l'air et certains matériaux tels que le verre. La longueur d'onde est une propriété importante de l'énergie électromagnétique. 1



Bien que les ondes radio, les micro-ondes, les ondes lumineuses visibles, les rayons x et les rayons gamma semblent être des éléments différents, ils sont tous des types d'énergie électromagnétique. Le classement de tous les types d'onde électromagnétique depuis l'onde la plus longue jusqu'à l'onde la plus courte forme un ensemble appelé spectre électromagnétique. 2


Noms
Puissance et téléphone
Ondes radioélectriques
Équipements
Générateurs tournants
Audiofréquences
Basses fréquences
Moyennes fréquences
Hautes fréquences
Tubes électroniques et équipements semi-
VHF (très hautes fréquences)
UHF (ultr hautes fréquence
Magnétrons, kly oscillateurs param et
Fréquence en hertz
Longueur d'onde en mètres
hertz
kilohertz
mégahertz
1
10
100
une seconde-lumière
diamètre de la terre
1 mégamètre
1 kilomètre
terrain de football
1 mètre

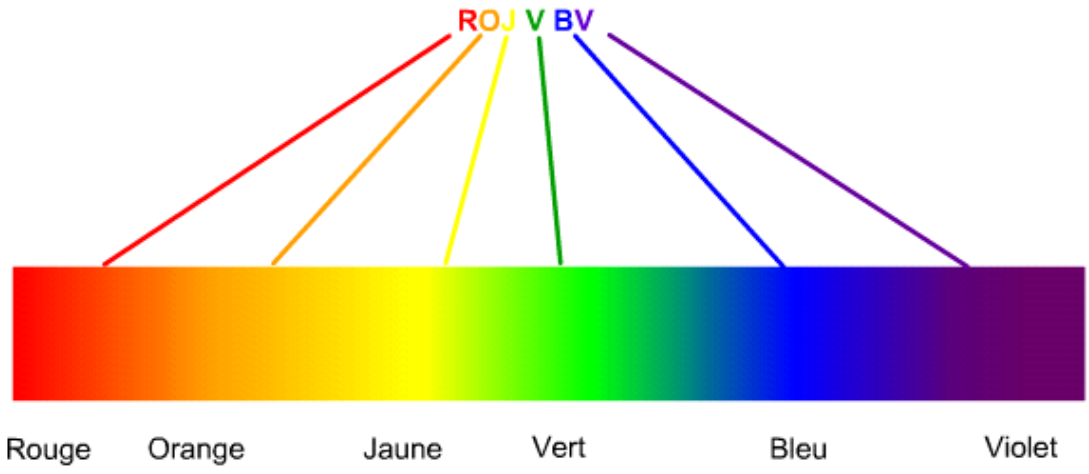
Micro-ondes
Infrarouge
LUMIÈRE
Ultraviolet
Rayons X
Ondes en centimétriques
Ondes en millimétriques
Sous-millimètre
Infrarouge lointain
Infrarouge intermédiaire
Lumière visible
Vide ultraviolet
Rayons X mous
Rayons X durs
Générateurs harmoniques et masers
Lampes à incandescence et à fluorescence, étincelles, arcs, tubes à décharge gazeuse et lasers
Tubes à rayons X électroniques et ioniques
Tubes à rayons X, isotopes radioactifs et générateurs de courant continu à haute tension
gigahertz
10
100
1
térahertz
10
100
1
1 millimètre
tête d'épingle
globule rouge
1 micromètre
virus de la polio
1 nanomètre
atome
1 angstrm
10^{9}
10^{10}
10^{11}
10^{12}
10^{13}
10^{14}
10^{15}
10^{16}
10^{17}
10^{18}
10^{19}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
10^{-11}



La longueur d'une onde électromagnétique est déterminée par le nombre de va-et-vient de l'onde générés par la charge électrique. Si la charge va et vient lentement, elle génère une onde longue. Le mouvement de la charge électrique est semblable à celui d'un bâton dans l'eau. Si le bâton va et vient lentement, il produit des ondulations dans l'eau avec une onde longue au sommet des ondulations. Si le mouvement du bâton s'accélère, les ondulations deviennent plus courtes.

Comme toutes les ondes électromagnétiques sont générées de la même manière, elles partagent un grand nombre de propriétés. Elles circulent toutes dans le vide à la même vitesse, soit approximativement à 300 000 kilomètres par seconde, qui est aussi la vitesse de la lumière.

L'œil humain ne perçoit que l'énergie électromagnétique avec des longueurs d'onde comprises entre 700 et 400 nanomètres. Un nanomètre équivaut à une longueur d'un milliardième de mètre (0,000000001 mètre). L'énergie électromagnétique dont la longueur d'onde est comprise entre 700 et 400 nanomètres est appelée lumière visible. Les ondes de lumière les plus longues avoisinant les 700 nanomètres sont de couleur rouge, et les ondes de lumière les plus courtes avoisinant les 400 nanomètres sont de couleur violette. Cette partie du spectre électromagnétique est semblable aux couleurs d'un arc-en-ciel. [3]



Les ondes non visibles par l'œil humain sont utilisées pour transmettre les données via la fibre optique. Ces ondes, légèrement plus longues que les ondes lumineuses rouges, sont les ondes lumineuses infrarouges utilisées notamment dans les télécommandes des téléviseurs. La lumière circulant dans la fibre optique a une longueur d'onde de 850, 1 310 ou 1 550 nanomètres. Ce sont les longueurs d'onde qui circulent le mieux dans la fibre optique.

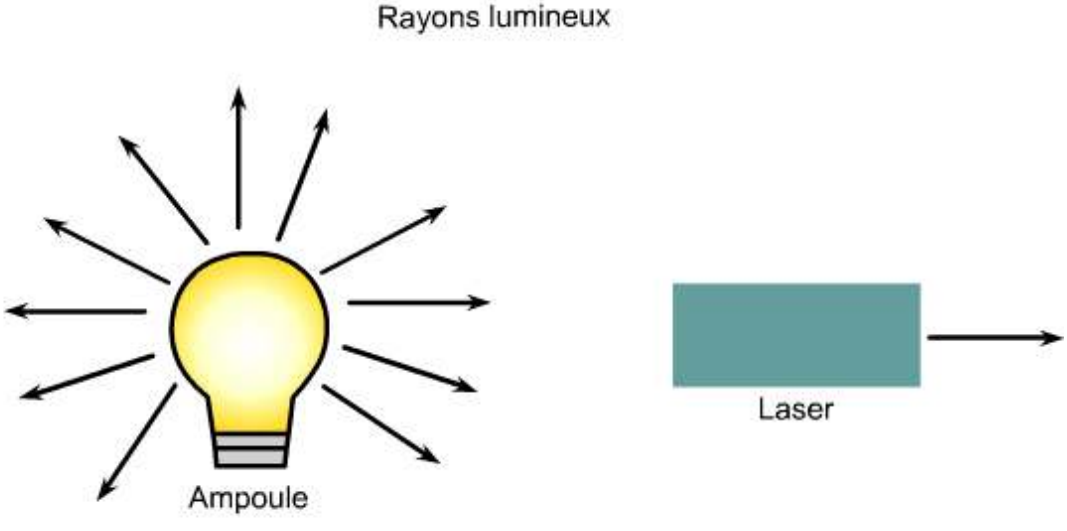
La page suivante décrit le modèle de rayons lumineux.

3.2 Médias optiques

3.2.2 Modèle de rayons lumineux

Cette page décrit les propriétés des rayons lumineux.

Les ondes électromagnétiques qui sortent d'une source forment des lignes droites appelées rayons. 1



$$\text{Indice de réfraction} = n = \frac{\text{Vitesse de la lumière dans le vide}}{\text{Vitesse de la lumière dans la matière}}$$

Ces rayons lumineux sont semblables aux faisceaux lumineux produits par les lasers. Dans le vide, la lumière circule en ligne droite continue à la vitesse de 300 000 kilomètres par seconde. Cependant, elle circule à des vitesses plus lentes dans des matières telles que l'air, l'eau et la glace. Lorsqu'un rayon lumineux, ou rayon incident, franchit la limite d'une matière pour pénétrer dans une autre matière, une partie de l'énergie lumineuse du rayon se réfléchit. C'est ainsi que votre image se reflète dans une vitre. La lumière ainsi réfléchie est appelée rayon réfléchi.

L'énergie lumineuse non réfléchie du rayon incident pénètre dans le verre. Le rayon entrant formant un angle par rapport à sa trajectoire d'origine est appelé rayon réfracté. L'amplitude de la flexion du rayon incident dépend de l'angle auquel il entre en contact avec la surface du verre et des vitesses auxquelles circule la lumière dans les deux matières.

La flexion des rayons lumineux à la limite des deux matières explique pourquoi ces rayons peuvent circuler dans une fibre optique même si elle est incurvée.

La densité optique du verre détermine l'amplitude de la flexion des rayons lumineux dans le verre. La densité optique mesure le ralentissement d'un rayon lumineux lorsqu'il pénètre dans une matière. Plus la densité optique d'une matière est élevée, plus elle ralentit la vitesse initiale de la lumière dans le vide. L'indice de réfraction est égal à la vitesse de la lumière dans le vide divisée par la vitesse de la lumière dans le média. Par conséquent, la mesure de la densité optique d'une matière correspond à l'indice de réfraction de cette matière. Une matière à indice de réfraction élevé est plus dense et ralentit plus la lumière qu'une matière à faible indice de réfraction. 2

Substance	Indice de réfraction
Air	1.000
Verre	1.523
Diamant	2.419
Eau	1.333

Il est possible d'augmenter l'indice de réfraction ou la densité optique du verre en ajoutant des substances chimiques. Plus le verre est pur, plus l'indice de réfraction est faible. Les leçons suivantes décrivent en détail la réflexion et la réfraction, ainsi que leur relation avec la conception et la fonction de la fibre optique.

L'activité de média interactive illustre la façon dont circule la lumière.

La page suivante décrit la réflexion.

Activité de média interactive

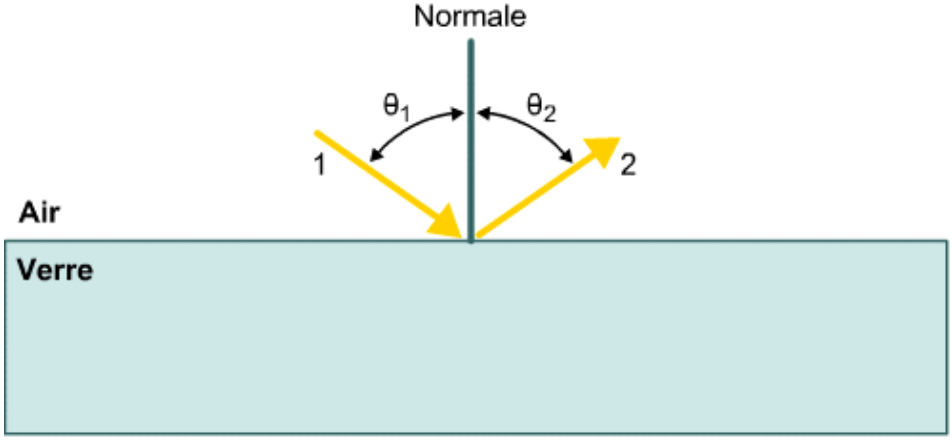
Interactivité: Propagation de la lumière dans la matière

Cette activité illustre le ralentissement de la vitesse de la lumière à travers différentes matières.

3.2 Médias optiques
3.2.3 Réflexion

Cette page décrit la réflexion.

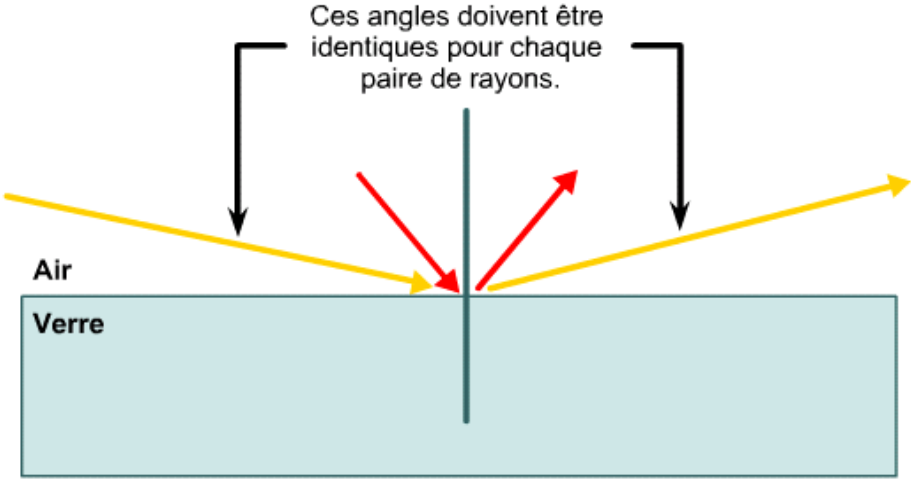
Lorsqu'un rayon lumineux (rayon incident) frappe la surface brillante d'un morceau de verre plat, une partie de l'énergie lumineuse du rayon se réfléchit. 1



Rayon 1 : Rayon incident, θ_1 degrés mesurés à partir de la normale
Rayon 2 : Rayon réfléchi, θ_2 degrés mesurés à partir de la normale
Loi de la réflexion : $\theta_1=\theta_2$

La lumière circulant dans l'air se réfléchit sur la surface du verre.

L'angle formé par le rayon incident et une ligne perpendiculaire à la surface du verre au point où le rayon frappe le verre est appelé angle d'incidence, et la ligne perpendiculaire est appelée ligne normale. Cette ligne n'est pas un rayon lumineux, mais un outil qui permet de mesurer les angles. L'angle formé par le rayon réfléchi et la ligne normale est appelé angle de réflexion. La loi de la réflexion stipule que l'angle de réflexion d'un rayon lumineux est égal à l'angle d'incidence. Autrement dit, l'angle auquel un rayon lumineux frappe une surface réfléchissante détermine l'angle de réflexion du rayon par rapport à la surface. 2



L'activité de média interactive illustre les lois de la réflexion.

La page suivante décrit la réfraction.

Activité de média interactive

Interactivité: Loi de la réflexion

Cette activité montre l'influence des angles sur la réflexion.

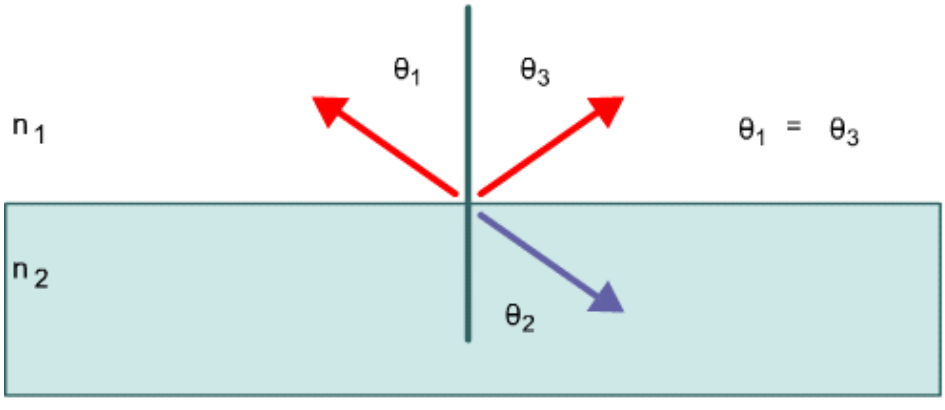
3.2 Médias optiques

3.2.4 Réfraction

Cette page décrit la réfraction.

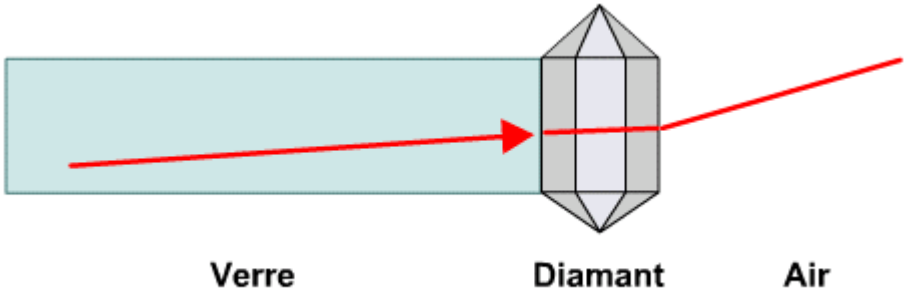
Lorsqu'un rayon lumineux frappe l'intervalle situé entre deux matières transparentes, la lumière se divise en deux parties. Une partie du rayon lumineux se reflète dans la première matière, avec un angle de réflexion égal à l'angle d'incidence. L'énergie restante du rayon traverse l'intervalle et pénètre dans la seconde matière.

Si le rayon incident frappe la surface du verre à exactement 90 degrés, il pénètre directement dans le verre et ne subit aucune flexion. Si l'angle n'est pas exactement égal à 90 degrés, le rayon entrant dans le verre se courbe et cette flexion est appelée réfraction. L'amplitude de réfraction du rayon dépend de l'indice de réfraction des deux matières transparentes. Si la lumière provient d'une matière dont l'indice de réfraction est plus faible que celui de la matière vers laquelle elle se dirige, le rayon réfracté se rapproche de la normale. Si la lumière provient d'une matière dont l'indice de réfraction est plus élevé que celui de la matière vers laquelle elle se dirige, le rayon réfracté s'éloigne de la normale. 1



$$n_1 \sin \theta_1 = n_2 \sin \theta_2$$

Supposons qu'un rayon lumineux franchisse la limite entre un morceau de verre et un diamant à un angle différent de 90 degrés. 2



L'index de réfraction du verre est d'environ 1,523 et celui du diamant est d'environ 2,419. Par conséquent, la trajectoire du rayon dans le diamant se rapprochera de la normale. Si le même rayon franchit la limite entre le diamant et l'air à un angle différent de 90 degrés, sa trajectoire s'éloignera de la normale car l'indice de réfraction de l'air est inférieur à celui du diamant d'environ 1,5.

L'activité de média interactive illustre le principe de réfraction.

La page suivante décrit le concept de réflexion interne totale.

Activité de média interactive

Interactivité: Réfraction optique

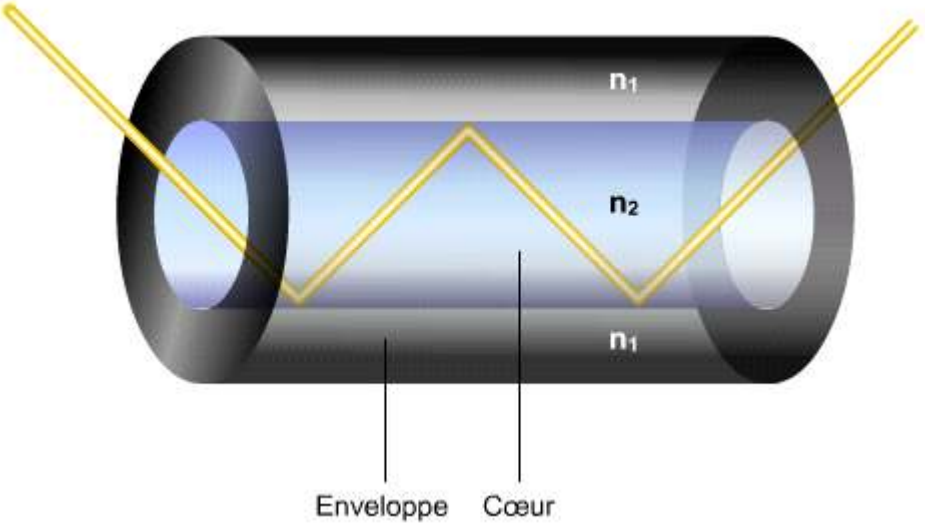
Cette activité illustre le mode de fonctionnement de la réfraction dans différentes matières.

3.2 Médias optiques

3.2.5 Réflexion interne totale

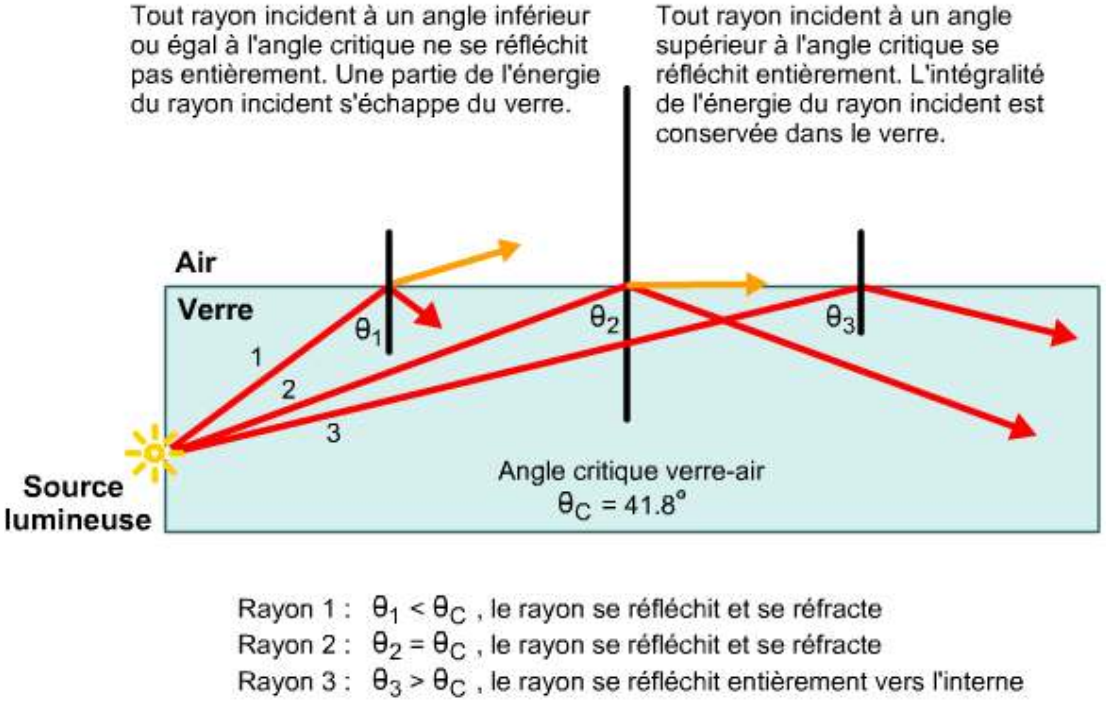
Cette page décrit le concept de réflexion interne totale dans le cadre des médias optiques.

Un rayon lumineux qui passe de l'état en fonction à l'état hors fonction (configuration de 1 et de 0) pour transmettre des données dans une fibre optique doit rester à l'intérieur de celle-ci jusqu'à ce qu'il atteigne son extrémité. Il ne doit pas se réfracter dans le matériau qui enveloppe la fibre, car la réfraction entraînerait la perte d'une partie de l'énergie lumineuse du rayon. La fibre doit être conçue de façon à ce que sa surface externe serve de miroir au rayon lumineux qui se déplace dans la fibre. Si tout rayon tentant de sortir de la fibre se réfléchissait dans la fibre à un angle qui l'achemine à l'extrémité de la fibre, il constituerait un bon conduit ou guide pour les ondes lumineuses. [1]



Les lois de réflexion et de réfraction illustrent la façon de concevoir une fibre guidant les ondes lumineuses qui la traversent avec un minimum de perte d'énergie. Les deux conditions suivantes doivent être remplies pour que les rayons lumineux se réfléchissent dans la fibre sans que la réfraction entraîne une perte d'énergie:

- L'indice de réfraction (n) au coeur de la fibre optique doit être supérieur à celui du matériau qui l'enveloppe. Le matériau protégeant le coeur de la fibre est appelé enveloppe.
- L'angle d'incidence du rayon lumineux est supérieur à l'angle critique du coeur et de son enveloppe.

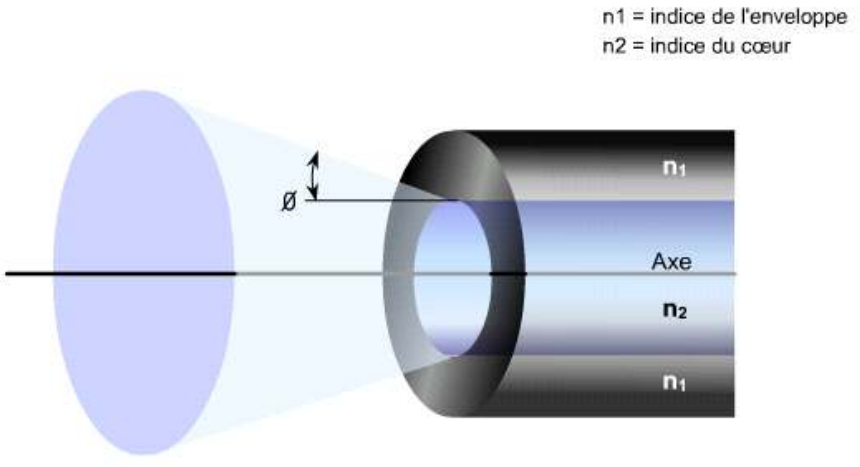

Tout rayon incident à un angle inférieur ou égal à l'angle critique ne se réfléchit pas entièrement. Une partie de l'énergie du rayon incident s'échappe du verre.
Tout rayon incident à un angle supérieur à l'angle critique se réfléchit entièrement. L'intégralité de l'énergie du rayon incident est conservée dans le verre.
Air
Verre
θ1
θ2
θ3
1
2
3
Source lumineuse
Angle critique verre-air
θC = 41.8°

Rayon 1 : $\theta_1 < \theta_C$, le rayon se réfléchit et se réfracte
Rayon 2 : $\theta_2 = \theta_C$, le rayon se réfléchit et se réfracte
Rayon 3 : $\theta_3 > \theta_C$, le rayon se réfléchit entièrement vers l'interne

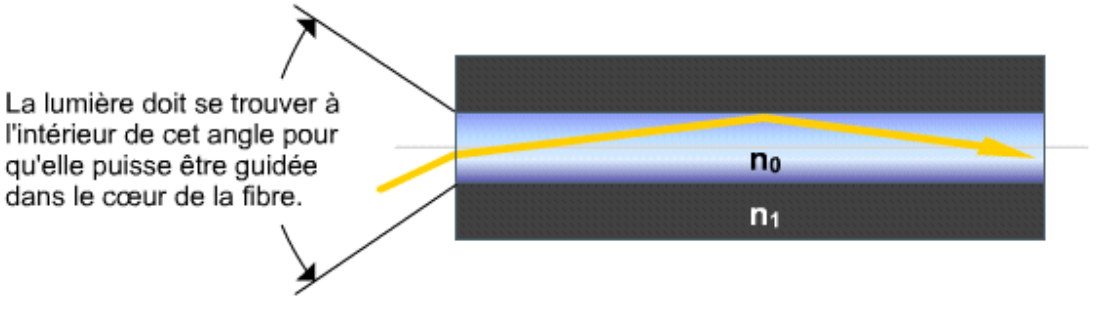
Si ces deux conditions sont remplies, l'intégralité du rayon incident se reflète à l'intérieur de la fibre. La conception d'une fibre optique repose sur ce principe appelé réflexion interne totale. La réflexion interne totale entraîne les rayons lumineux circulant dans la fibre hors de la limite cœur-enveloppe et les achemine vers l'extrémité de la fibre. La lumière franchit le coeur de la fibre en zigzag.

Il est facile de fabriquer une fibre qui remplit la première condition. En outre, il est possible de contrôler l'angle d'incidence des rayons lumineux entrant dans le cœur en limitant les deux facteurs suivants:

- **Ouverture numérique de la fibre** – L'ouverture numérique d'un coeur est l'intervalle des angles des rayons incidents pénétrant dans la fibre qui seront entièrement réfléchis.
- **Modes** – Chemins suivis par un rayon lumineux lorsqu'il se déplace dans une fibre. 3 4



L'ouverture numérique mesure la plage d'angles qui se réfléchira totalement en interne



Le contrôle de ces deux facteurs permet d'obtenir une réflexion interne totale au cours du déplacement de rayons lumineux dans une fibre. Les ondes lumineuses disposent ainsi d'un guide qui peut être utilisé dans la communication de données.

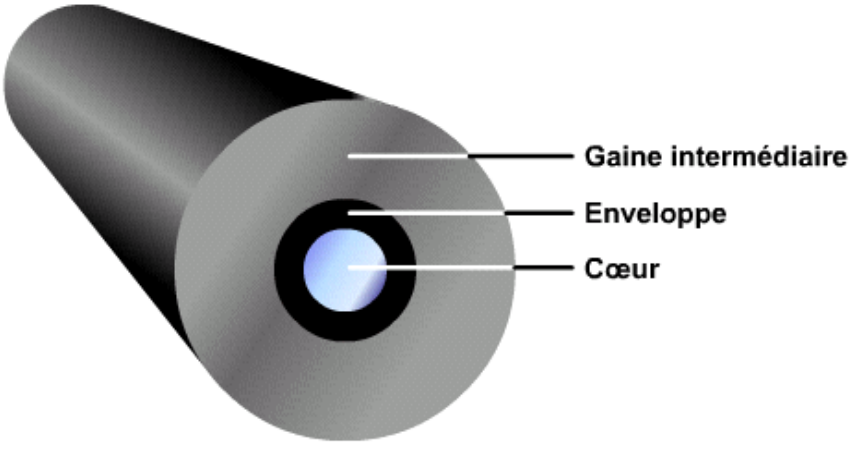
La page suivante traite de la fibre multimode.

3.2 Médias optiques

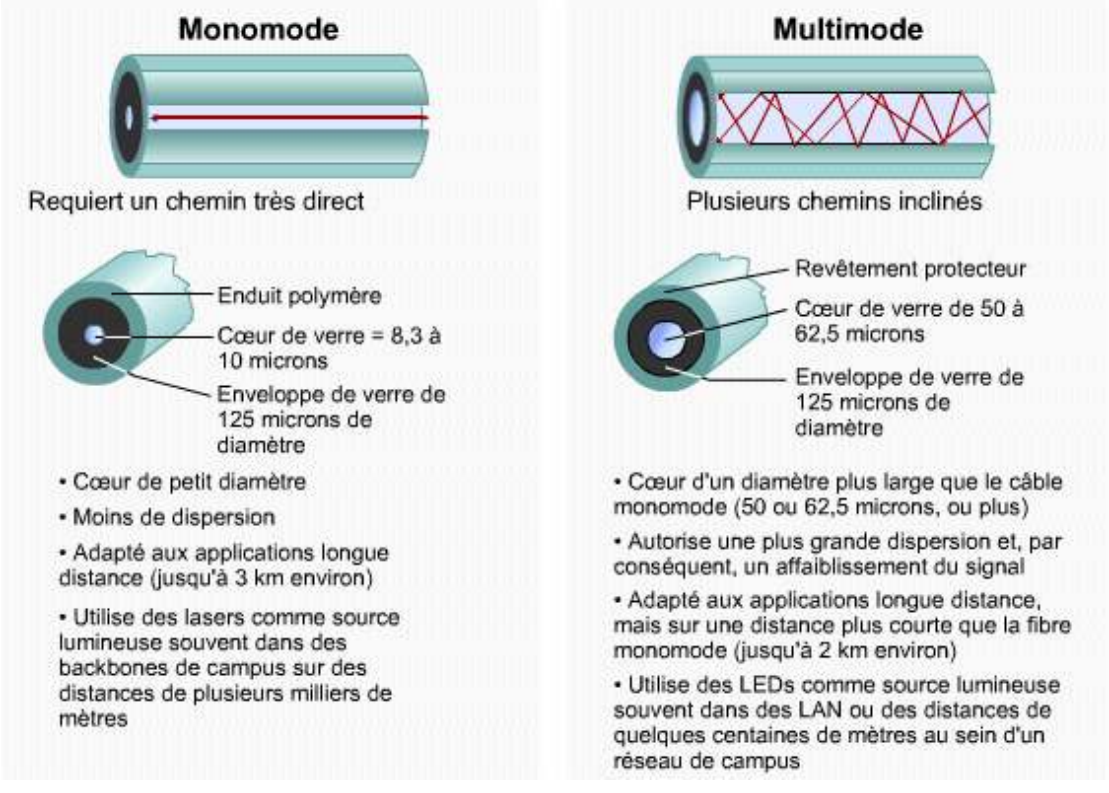
3.2.6 Fibre multimode

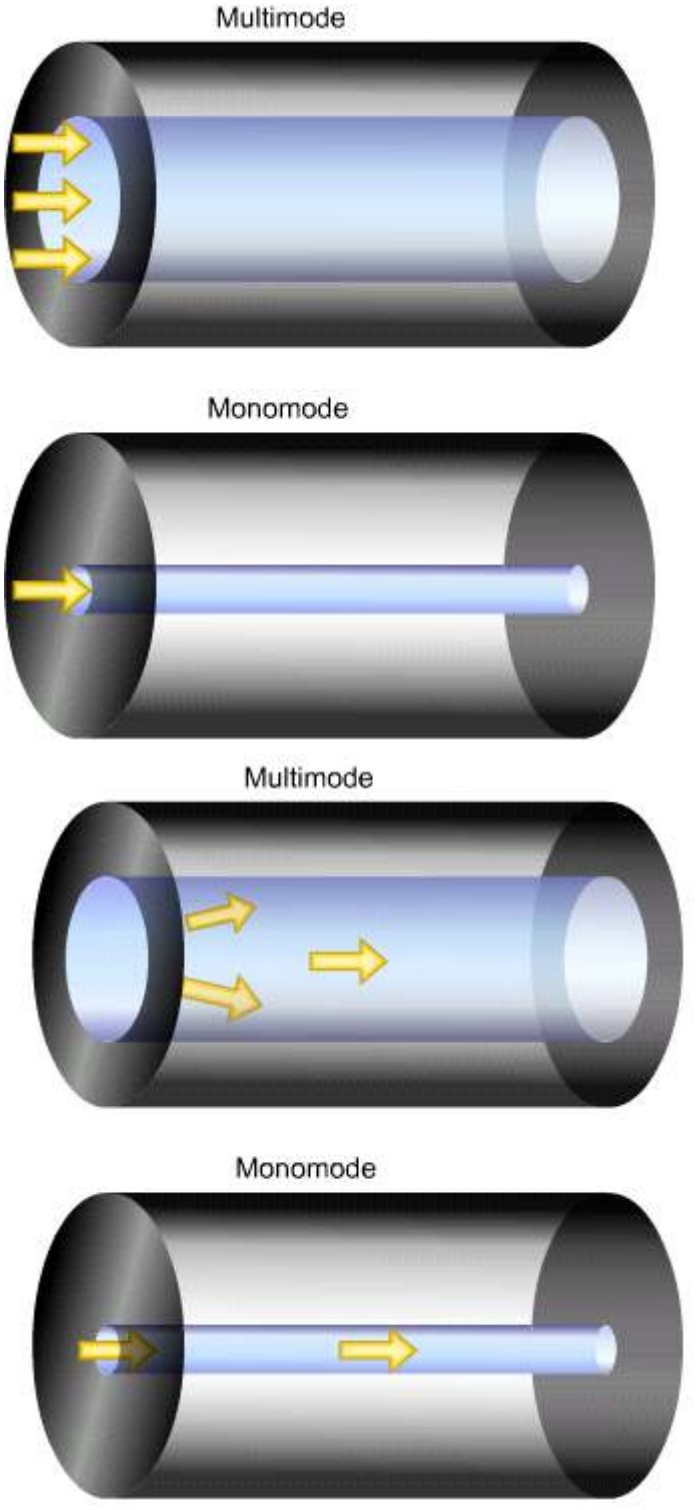
Cette page présente la fibre multimode.

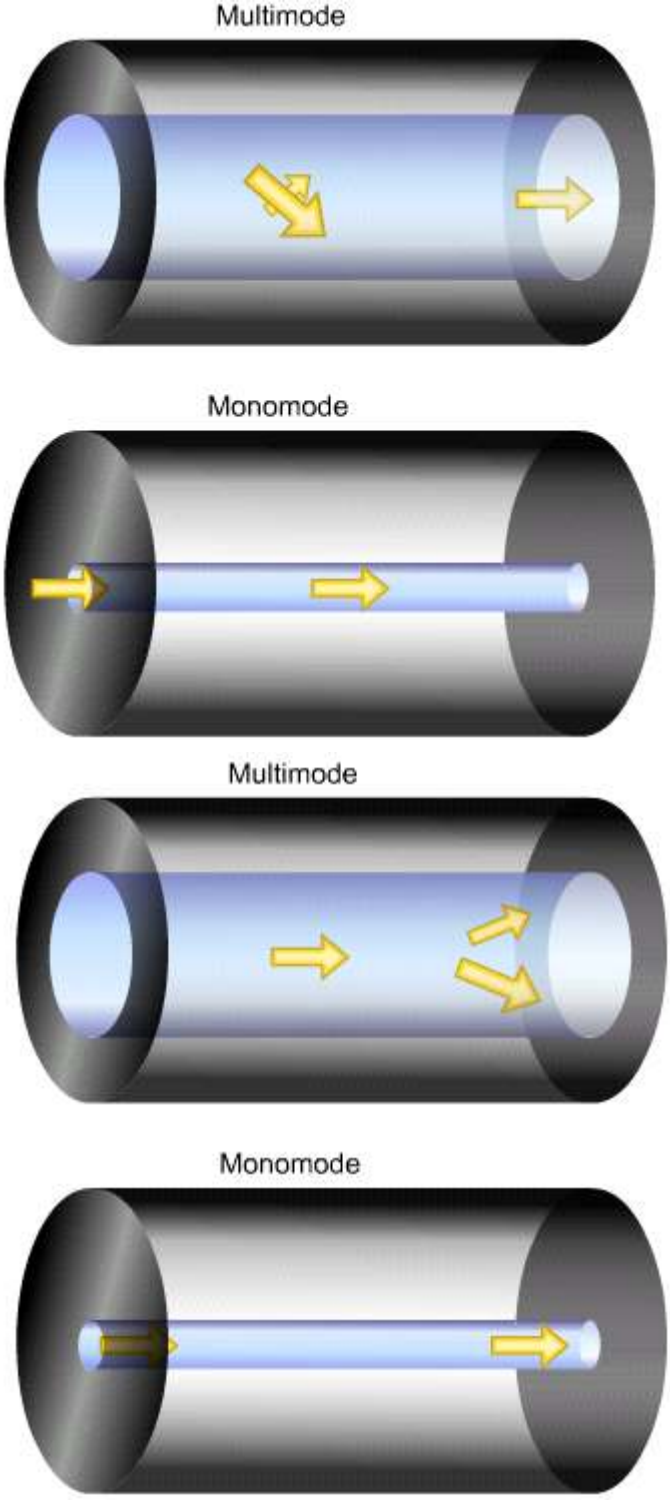
Le coeur d'une fibre optique est la partie dans laquelle circulent les rayons lumineux. 1

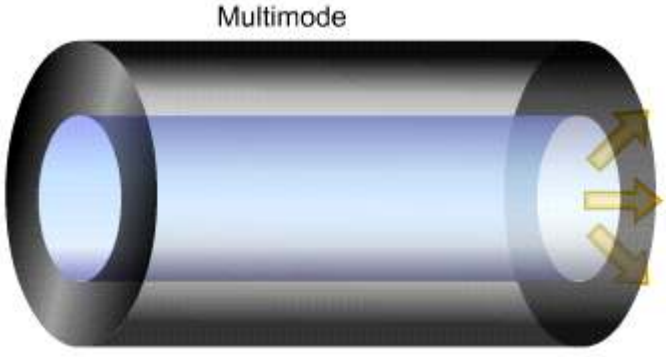


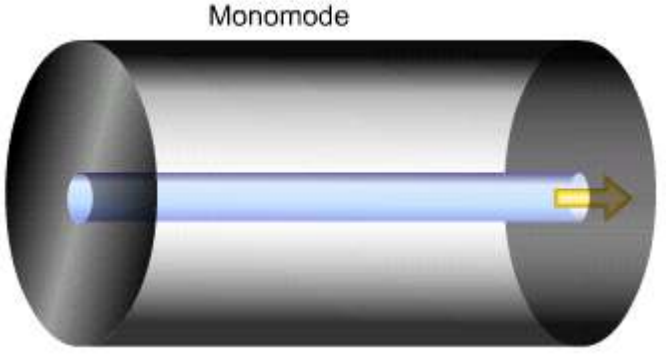
Un rayon lumineux ne peut pénétrer dans le coeur que si son angle est compris dans l'ouverture numérique de la fibre. De même, une fois dans le coeur de la fibre, un rayon lumineux ne peut suivre qu'un nombre limité de chemins optiques. Ces chemins sont appelés modes. Si le diamètre du coeur de la fibre est suffisamment large de façon à ce que la lumière puisse suivre plusieurs chemins à l'intérieur de la fibre, celle-ci est appelée fibre multimode. En revanche, les rayons lumineux ne disposent que d'un seul mode pour circuler au coeur d'une fibre monomode dont le diamètre est plus petit. [2] [3]


Monomode
Requiert un chemin très direct
Enduit polymère
Cœur de verre = 8,3 à 10 microns
Enveloppe de verre de 125 microns de diamètre
• Cœur de petit diamètre
• Moins de dispersion
• Adapté aux applications longue distance (jusqu'à 3 km environ)
• Utilise des lasers comme source lumineuse souvent dans des backbones de campus sur des distances de plusieurs milliers de mètres
Multimode
Plusieurs chemins inclinés
Revêtement protecteur
Cœur de verre de 50 à 62,5 microns
Enveloppe de verre de 125 microns de diamètre
• Cœur d'un diamètre plus large que le câble monomode (50 ou 62,5 microns, ou plus)
• Autorise une plus grande dispersion et, par conséquent, un affaiblissement du signal
• Adapté aux applications longue distance, mais sur une distance plus courte que la fibre monomode (jusqu'à 2 km environ)
• Utilise des LEDs comme source lumineuse souvent dans des LAN ou des distances de quelques centaines de mètres au sein d'un réseau de campus

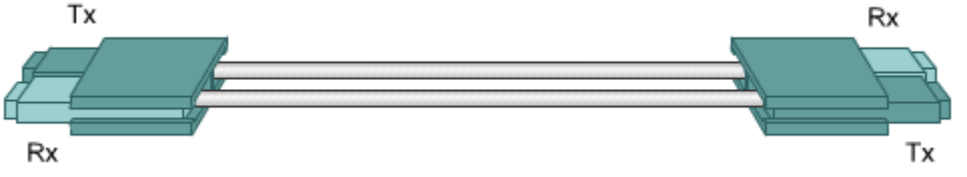

Multimode
Monomode
Multimode
Monomode


Multimode
Monomode
Multimode
Monomode



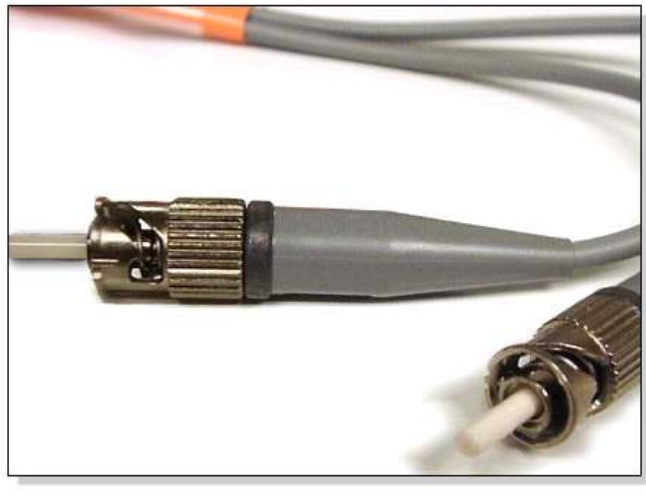


Chaque câble à fibre optique utilisé dans les réseaux comprend deux fibres de verre logées dans des enveloppes distinctes. Une fibre transporte les données transmises depuis l'équipement A vers l'équipement B [4]



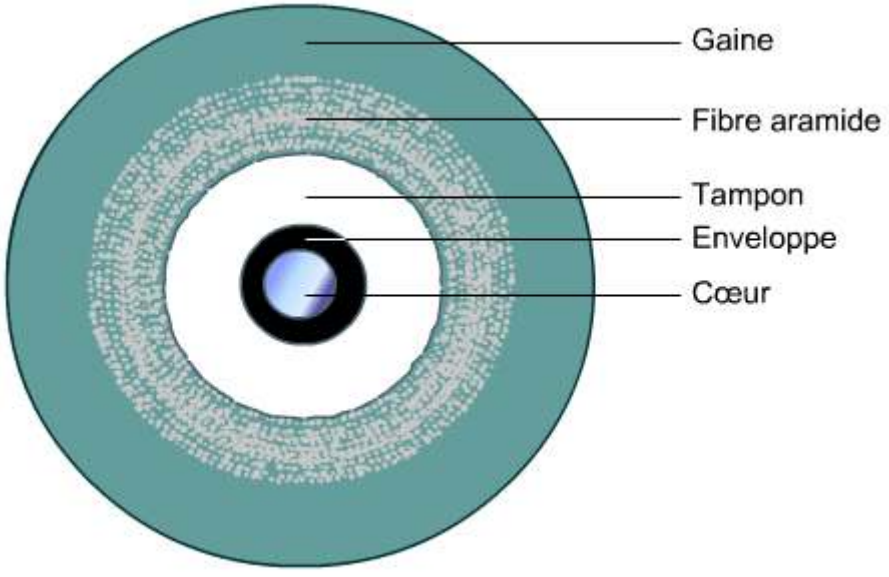
, et l'autre depuis l'équipement B vers l'équipement A. Les fibres sont similaires à deux rues en sens unique dont la direction est opposée. Elles assurent ainsi une liaison de communication full duplex. Les médias de cuivre à paires torsadées utilisent une paire de fils pour la transmission et une autre paire pour la réception. Les circuits à fibre optique utilisent un brin de fibre pour la transmission et un autre pour la réception. En général, ces deux fibres sont enveloppées ensemble par une gaine externe jusqu'au point auquel elles sont reliées aux connecteurs. [5]

Aucun blindage n'est nécessaire jusqu'aux connecteurs, car la lumière ne s'échappe pas une fois à l'intérieur d'une fibre. Autrement dit, les fibres ne génèrent aucun problème de diaphonie. Il est très courant de loger plusieurs paires de fibres dans le même câble, ce qui permet d'installer un seul câble entre des locaux de câblage, des étages ou des bâtiments. Un câble peut contenir de 2 à 48 fibres séparées (ou plus), alors qu'un câble de cuivre UTP doit être installé pour chaque circuit. La fibre optique peut transporter plus de bits par seconde et sur une distance plus



longue que le média de cuivre.

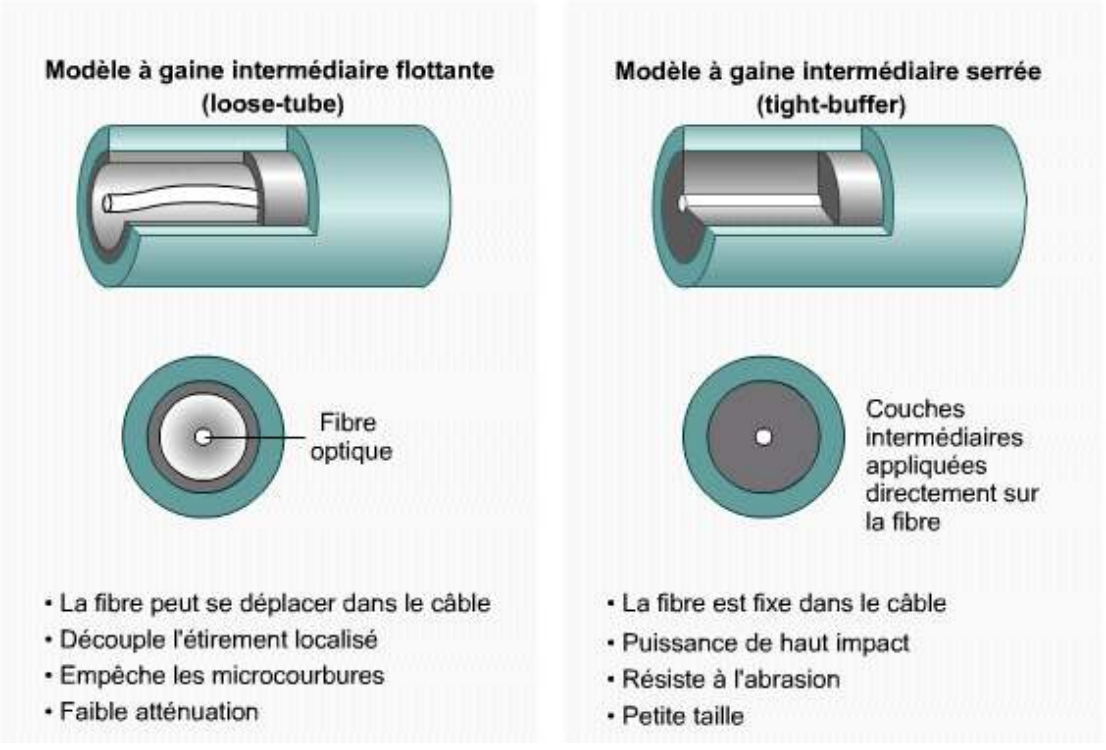
En général, un câble à fibre optique comprend cinq éléments : le coeur, l'enveloppe, une gaine intermédiaire, un matériau de résistance et une gaine externe. 6



Le coeur constitue l'élément de transmission de la lumière au centre de la fibre optique. Tous les signaux lumineux circulent dans le coeur. Il est généralement fabriqué dans un type de verre alliant l'oxyde de silicium et d'autres éléments. Le coeur des fibres multimodes est fabriqué dans un verre à gradient d'indice qui offre un indice de réfraction faible vers le bord externe du coeur. Par conséquent, le bord externe du coeur étant optiquement moins dense que le centre, la lumière circule plus vite dans cette partie externe. Ce principe de conception est nécessaire car un rayon lumineux suivant un mode qui l'achemine directement au centre du cœur n'a pas à parcourir une distance aussi longue que s'il suivait un mode qui le fasse rebondir en périphérie du cœur dans la fibre. Tous les rayons doivent parvenir ensemble à l'extrémité de la fibre et le récepteur situé à l'extrémité reçoit un flash de lumière intense au lieu d'une impulsion longue et faible.

L'enveloppe qui entoure le coeur contient également de l'oxyde de silicium mais son indice de réfraction est moins élevé que celui du coeur. Les rayons lumineux gravitant autour du coeur de la fibre se réfléchissent sur l'intervalle compris entre le coeur et l'enveloppe lorsqu'ils circulent dans la fibre par réflexion interne totale. Le câble à fibre optique multimode standard est le type de câble optique le plus utilisé dans les réseaux locaux. Il utilise une fibre optique avec un coeur d'un diamètre de 62,5 ou 50 microns et une enveloppe d'un diamètre de 125 microns. Il est souvent appelé câble à fibre optique de 62,5/125 ou 50/125 microns. Un micron équivaut à un millionième de mètre (1µ).

Une gaine intermédiaire, généralement en matière plastique, entoure l'enveloppe. Elle protège le coeur et l'enveloppe contre tout dommage. Il existe deux modèles de câble: le modèle à gaine intermédiaire flottante (loose-tube) et le modèle à gaine intermédiaire serrée (tight-buffered). 7


Modèle à gaine intermédiaire flottante
(loose-tube)
Fibre optique
• La fibre peut se déplacer dans le câble
• Découple l'étirement localisé
• Empêche les microcourbures
• Faible atténuation
Modèle à gaine intermédiaire serrée
(tight-buffer)
Couches intermédiaires appliquées directement sur la fibre
• La fibre est fixe dans le câble
• Puissance de haut impact
• Résiste à l'abrasion
• Petite taille

La plupart des câbles à fibre optique utilisés dans les réseaux locaux sont des câbles à gaine intermédiaire serrée. Celle-ci est en contact direct avec l'enveloppe. La différence entre les deux modèles réside principalement dans leur utilisation : les modèles à gaine intermédiaire flottante sont surtout utilisés à l'extérieur des bâtiments, alors que les modèles à gaine intermédiaire serrée sont utilisés à l'intérieur des bâtiments.

Le matériau de résistance entourant la gaine intermédiaire empêche le câble de fibre de s'étirer au cours des installations. Le matériau utilisé est souvent la fibre aramide (Kevlar), qui sert également à fabriquer les gilets pare-balles.

La gaine externe est le dernier élément d'un câble à fibre optique. Elle enveloppe la fibre pour la protéger contre l'abrasion, les solvants et autres contaminants. La couleur de la gaine externe d'une fibre multimode est généralement orange, mais elle peut être d'une autre couleur.

Les LED *(Light Emitting Diodes)* ou les lasers VCSEL *(Vertical Cavity Surface Emitting Lasers)* infrarouges sont les deux types de source lumineuse généralement utilisés avec la fibre multimode. Vous pouvez utiliser l'un ou l'autre. Les LED sont moins onéreuses et requièrent moins de précautions d'utilisation que les lasers VCSEL. Cependant, elles ne transmettent pas la lumière aussi loin que les lasers. Une fibre multimode (62,5/125) peut transporter des données jusqu'à une distance de 2 000 mètres.

La page suivante décrit la fibre monomode.

3.2 Médias optiques

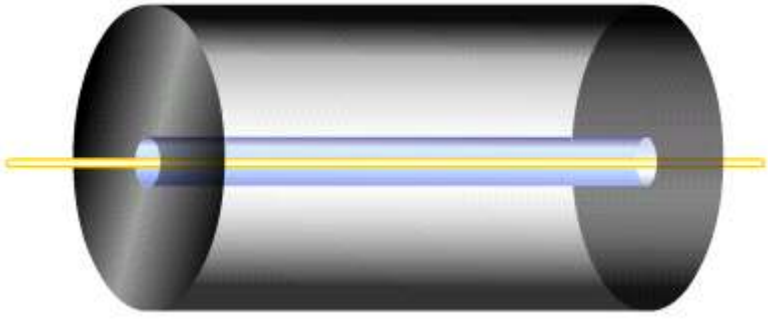
3.2.7 Fibre monomode

Cette page présente la fibre monomode.

La fibre monomode comprend les mêmes composants que la fibre multimode. La gaine externe de la fibre monomode est généralement de couleur jaune. La principale différence entre la fibre multimode et la fibre

monomode réside dans le fait que cette dernière n'autorise qu'un seul mode de propagation de la lumière à travers le coeur d'un diamètre de huit à dix microns (les cœurs de neuf microns sont les plus répandus). La marque 9/125 visible sur la gaine d'une fibre monomode indique le diamètre du coeur (9 microns) et celui de l'enveloppe (125 microns).

Une fibre monomode utilise un laser infrarouge comme source lumineuse. Le rayon lumineux qu'il génère pénètre dans le coeur à un angle de 90 degrés. Par conséquent, les données transportant les impulsions du rayon lumineux dans une fibre monomode sont essentiellement transmises en ligne droite directement au centre du coeur, 1

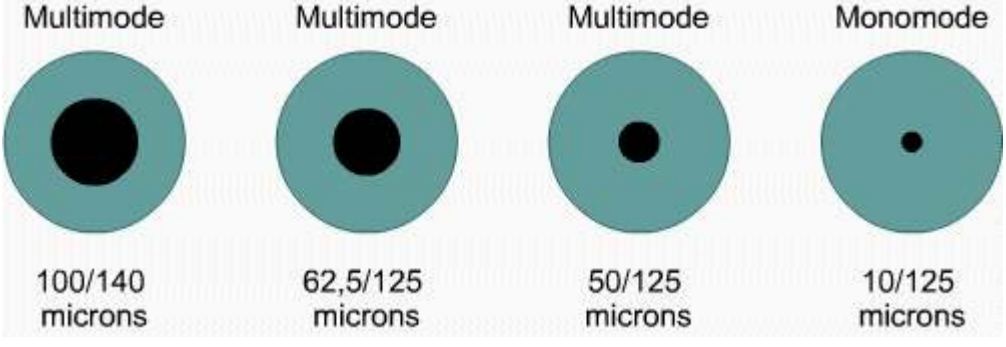


ce qui accroît considérablement la vitesse et la distance de transmission des données.

En raison de sa conception, la fibre monomode prend en charge des débits de données (bande passante) plus élevés et des distances plus longues que la fibre multimode. La fibre monomode peut transporter des données jusqu'à 3 000 mètres dans un réseau local. Bien que cette distance soit considérée comme une norme, de nouvelles technologies (traitées dans un prochain module) l'ont accrue. La fibre multimode ne peut transporter des données que sur 2 000 mètres maximum. Les fibres monomodes et les lasers sont plus onéreux que les fibres multimodes et les LED. En raison de toutes ces caractéristiques, la fibre monomode est souvent utilisée pour assurer la connectivité entre bâtiments.

Avertissement : Le laser utilisé avec la fibre monomode génère une longueur d'onde visible. Le rayon laser est si puissant qu'il peut provoquer de graves lésions oculaires. **Ne** regardez **jamais** l'extrémité libre d'une fibre dont l'autre extrémité est connectée à un équipement. **Ne** regardez **jamais** le port de transmission d'une carte réseau, d'un commutateur ou d'un routeur. Veillez à conserver le protecteur isolant sur les extrémités du câble et dans les ports à fibre optique des commutateurs et des routeurs. Procédez avec prudence.

La figure 2



compare les tailles relatives du coeur et de l'enveloppe des deux types de fibre optique sous différentes coupes. La fibre monomode prend en charge une bande passante plus large et une distance plus longue que la fibre multimode en raison de son coeur qui est plus petit et plus affiné. Cependant, son coût de fabrication est plus élevé.

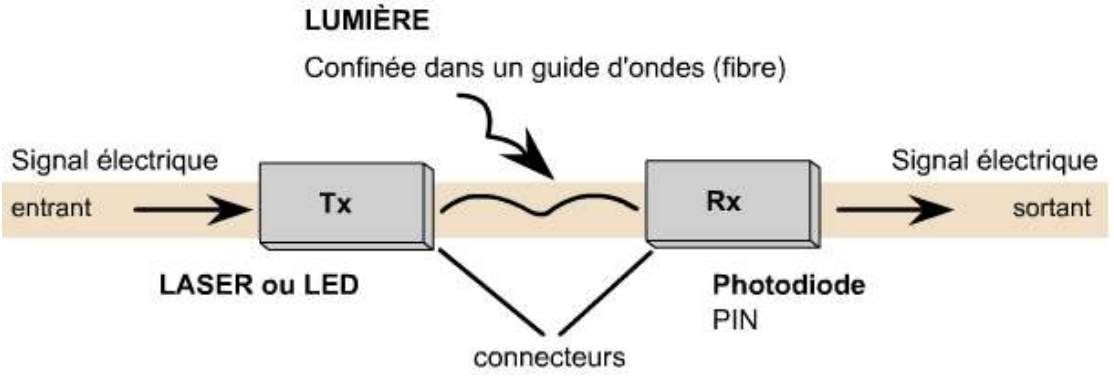
La page suivante présente certains équipements utilisés avec la fibre optique.

3.2 Médias optiques

3.2.8 Autres équipements optiques

Cette page explique comment utiliser certains équipements optiques pour transmettre des données.

Dans un réseau local, la plupart des données sont envoyées sous la forme de signaux électriques. Comme les liaisons à fibre optique utilisent la lumière pour envoyer des données, il est nécessaire de convertir l'électricité en lumière à une extrémité de la fibre et de reconvertir la lumière en électricité à l'autre extrémité. C'est la raison pour laquelle un émetteur et un récepteur sont nécessaires. 1



L'émetteur reçoit des commutateurs et des routeurs les données à transmettre sous la forme de signaux électriques, puis convertit ces derniers en impulsions lumineuses équivalentes. Deux types de source lumineuse permettent de coder et de transmettre les données via le câble:

- Une diode électroluminescente (LED) produisant une lumière infrarouge avec des longueurs d'onde de 850 ou 1 310 nanomètres, utilisée avec la fibre multimode dans les réseaux locaux. Des lentilles permettent de concentrer la lumière infrarouge sur l'extrémité de la fibre.
- Un laser *(Light Amplification by Stimulated Emission Radiation)* produisant un faisceau étroit de lumière infrarouge intense avec des longueurs d'onde de 1 310 ou 1 550 nanomètres, utilisé avec la fibre monomode sur de longues distances dans des réseaux WAN ou des backbones de campus. Cette méthode exige des précautions pour éviter toute lésion oculaire.

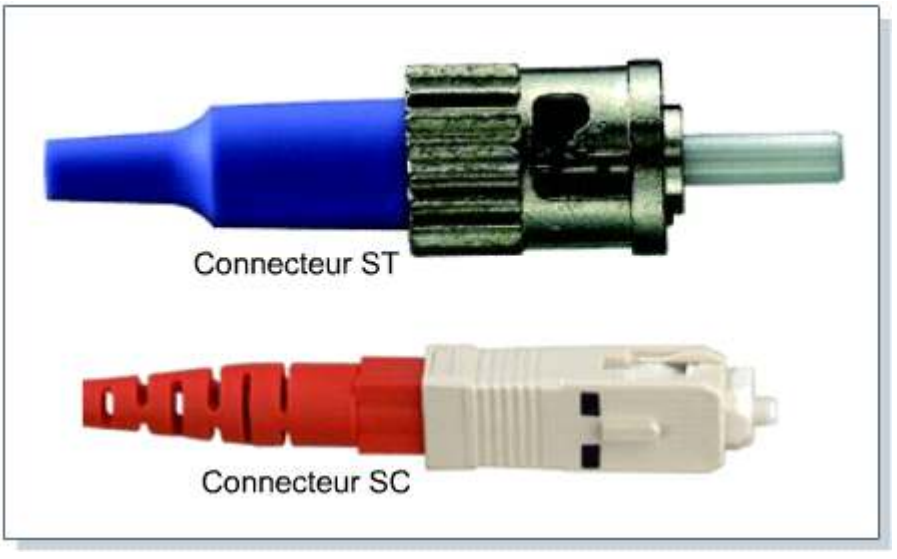
Il est possible d'augmenter ou de diminuer très rapidement l'intensité lumineuse de chacune de ces sources pour envoyer les données (1 et 0) à un nombre élevé de bits par seconde.

Le récepteur est placé à l'autre extrémité de la fibre optique. Il fonctionne d'une façon similaire à celle d'une photopile dans une calculatrice. Lorsque la lumière atteint le récepteur, elle produit de l'électricité. Après avoir détecté une impulsion lumineuse en provenance de la fibre, le récepteur la reconvertit dans le signal électrique d'origine sous la forme duquel elle est entrée initialement dans l'émetteur à l'autre extrémité de la fibre. Le signal est de nouveau soumis aux variations de tension, prêt à être envoyé via un fil de cuivre dans n'importe quel récepteur électronique tel qu'un ordinateur, un commutateur ou un routeur. Les photodiodes PIN (p-intrinsic-n diodes) sont des équipements semi-conducteurs généralement utilisés comme récepteurs avec des liaisons optiques.

Ces récepteurs sont conçus pour être sensibles aux longueurs d'onde de 850, 1 310 ou 1 550 nanomètres générées par l'émetteur à l'autre extrémité de la fibre. Lorsqu'une impulsion lumineuse de cet ordre de grandeur entre en contact avec une photodiode PIN, celle-ci produit rapidement du courant électrique à une tension appropriée au réseau. Elle arrête instantanément de produire cette tension dès qu'il n'existe plus d'impulsion lumineuse, ce qui génère des variations de tension représentées par des 1 et des 0 sur un câble de cuivre.

Des connecteurs sont reliés aux extrémités des fibres de sorte qu'il soit possible de connecter celles-ci aux ports de l'émetteur et du récepteur. Les connecteurs les plus fréquemment utilisés sont les connecteurs SC (*Subscriber Connector*) pour la fibre multimode, et les connecteurs ST *(Straight Tip)* pour la fibre monomode. [2] [3]

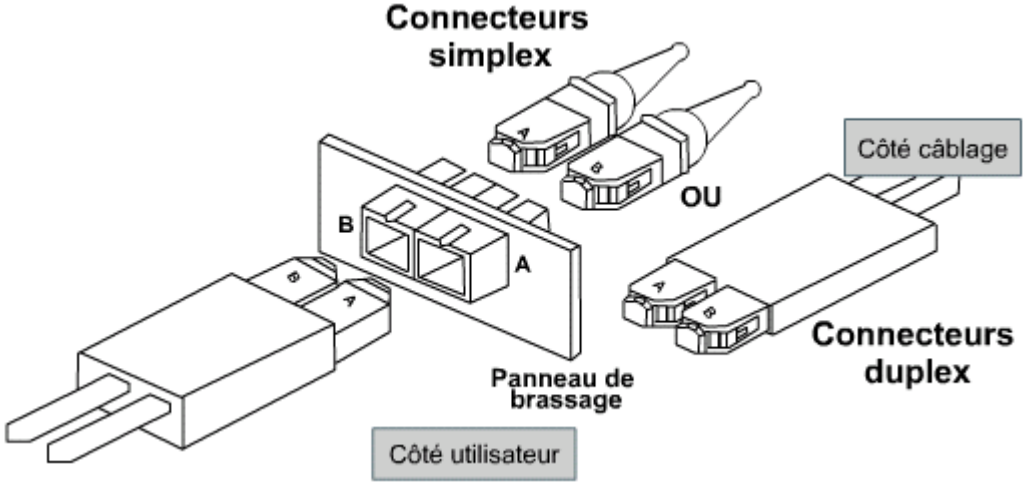


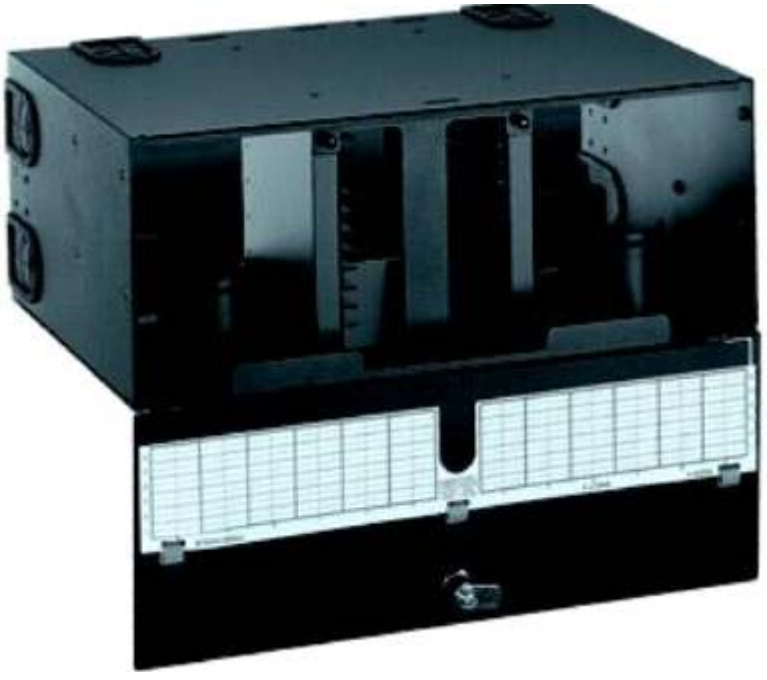


Outre les émetteurs, récepteurs, connecteurs et fibres qui sont toujours indispensables dans un réseau optique, les répéteurs et les panneaux de brassage sont d'autres médias optiques souvent utilisés.

Les répéteurs et les amplificateurs optiques qui reçoivent des impulsions lumineuses s'atténuant sur de longues distances rétablissent leur forme d'origine, leur puissance et leur synchronisation. Les signaux restaurés peuvent ensuite être transmis au récepteur qui se trouve à l'autre extrémité de la fibre.

Les panneaux de brassage optiques sont similaires à ceux utilisés avec les câbles en cuivre. Ils améliorent la souplesse d'un réseau optique car ils permettent de modifier rapidement la connexion des équipements (commutateurs, routeurs, etc.). [4] [5]





L'activité de TP est consacrée au prix des différents types de câble à fibre optique.

La page suivante décrit la perte de données dans les câbles à fibre optique.

Activité de TP

Exercice: Achat de câbles à fibre optique

Ce TP présente les différents composants et câbles réseau disponibles sur le marché, ainsi que leurs prix. Les étudiants vont collecter des informations sur les tarifs des câbles de raccordement et en vrac à fibre optique.

3.2 Médias optiques

3.2.9 Signaux et bruit dans les médias à fibre optique

Cette page décrit certains facteurs qui contribuent à réduire la puissance des signaux dans un média optique.

Les câbles à fibre optique ne sont pas affectés par les mêmes sources de bruit externe qui engendrent des problèmes sur les médias de cuivre, car la lumière externe ne peut pas pénétrer dans la fibre, excepté à l'extrémité où se trouve l'émetteur. L'enveloppe de la fibre est protégée par une gaine intermédiaire et une gaine externe qui empêchent la lumière de pénétrer dans le câble ou de s'en échapper.

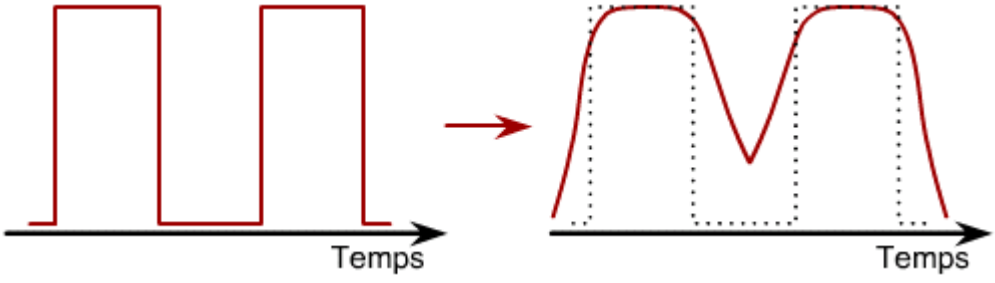
En outre, la transmission de la lumière dans une fibre d'un câble ne génère aucune interférence susceptible de perturber la transmission dans une autre fibre du câble. Autrement dit, les problèmes de diaphonie présents dans les câbles de cuivre n'existent pas dans les câbles optiques. La qualité des liaisons optiques est telle que les dernières normes Gigabit Ethernet et 10 Gibabit Ethernet spécifient des distances de transmission nettement supérieures aux deux kilomètres traditionnels de la norme Ethernet initiale. La transmission via un média optique permet d'utiliser le protocole Ethernet sur des réseaux métropolitains et longue distance.

Si la fibre est considérée comme le média de transmission le meilleur pour transporter de grandes quantités de données sur de longues distances, elle présente néanmoins quelques problèmes. Lorsque la lumière circule dans la fibre, elle perd de son énergie. Plus la distance à parcourir est longue, plus la puissance du signal diminue. Cette atténuation est due à plusieurs facteurs inhérents à la fibre, dont le plus important est la dispersion. La dispersion de la lumière dans une fibre est provoquée par des inégalités microscopiques (distorsions) qui réfléchissent et dispersent l'énergie lumineuse.

L'absorption est une autre cause de perte d'énergie. Lorsqu'un rayon lumineux entre en contact avec certaines impuretés dans une fibre, celles-ci absorbent une partie de l'énergie qui est convertie en une petite quantité d'énergie thermique, ce qui affaiblit le signal lumineux.

Les rugosités ou les défauts de fabrication présents entre le coeur et l'enveloppe d'une fibre constituent un autre facteur d'atténuation des signaux lumineux. Ces derniers perdent de leur puissance en raison de la réflexion interne totale qui se dégrade dans cette zone. Toute imperfection microscopique au niveau de l'épaisseur ou de la symétrie de la fibre diminue la réflexion interne totale et entraîne l'absorption d'une partie de l'énergie lumineuse par l'enveloppe.

La dispersion d'un flash de lumière limite également les distances de transmission dans une fibre. La dispersion est le terme technique utilisé pour désigner la propagation des impulsions lumineuses qui circulent dans une fibre. 1



La fibre multimode à gradient d'indice est conçue pour compenser les différentes distances que doivent parcourir les différents modes dans le diamètre large du coeur. Même si ce problème n'existe pas avec la fibre monomode, la dispersion chromatique est néanmoins une caractéristique des fibres multimodes et monomodes. La circulation de longueurs d'onde à des vitesses différentes dans le verre engendre la dispersion chromatique. C'est pourquoi les longueurs d'onde sont séparées par un prisme. Idéalement, si une diode électroluminescente ou un laser émettait la lumière d'une seule fréquence, la dispersion chromatique ne poserait aucun problème.

Cependant, comme les lasers, et particulièrement les diodes électroluminescentes génèrent une plage de longueurs d'onde, la dispersion chromatique limite la distance de transmission dans une fibre. Si un signal est transmis trop loin, l'impulsion d'énergie lumineuse initialement intense, se disperse, se sépare et s'affaiblit lorsque le signal atteint le récepteur, et ce dernier ne parvient plus à distinguer un 1 d'un 0.

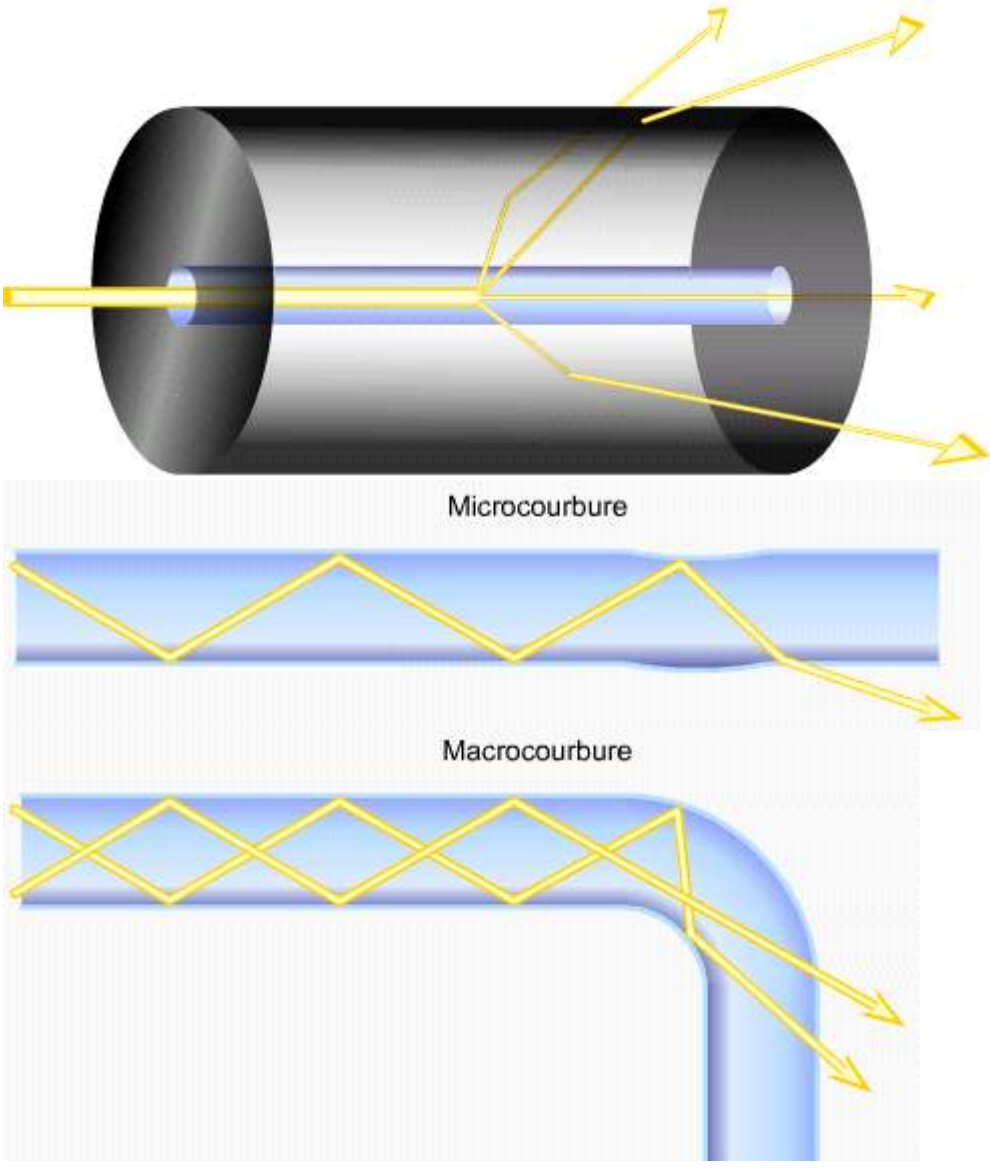
La page suivante décrit l'installation, l'entretien et la vérification des câbles à fibre optique.

3.2 Médias optiques

3.2.10 Installation, entretien et vérification des câbles à fibre optique

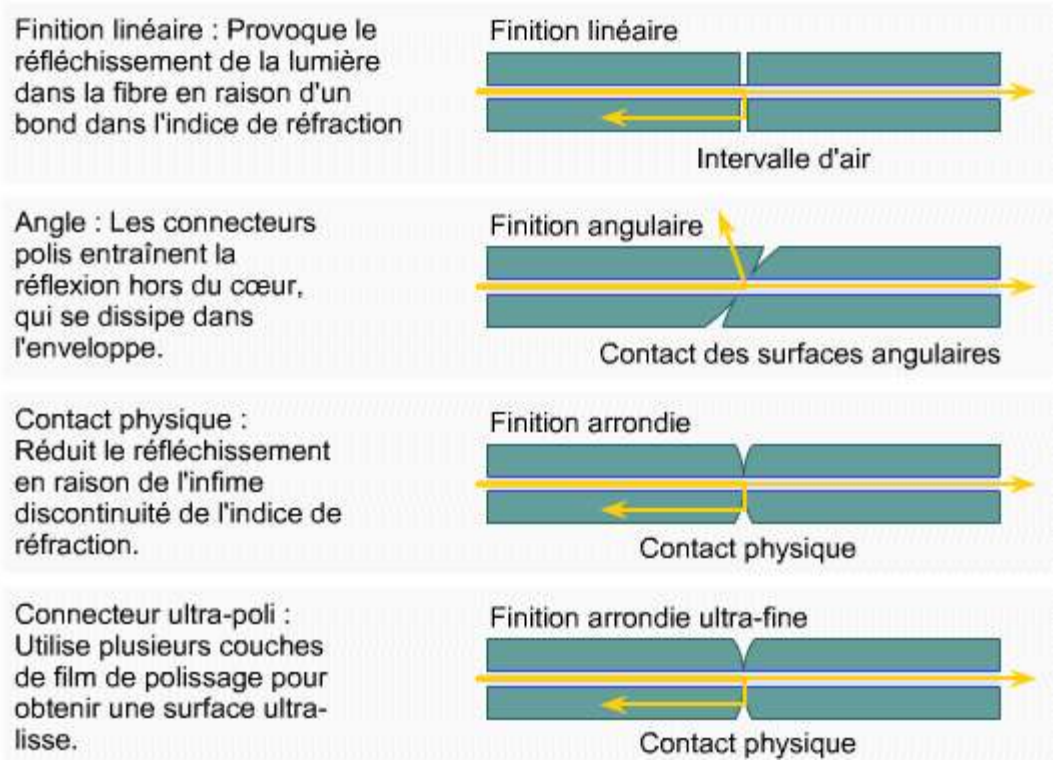
Cette page explique comment résoudre les problèmes liés aux câbles à fibre optique.

Une installation incorrecte est une des principales causes d'une atténuation excessive dans un câble à fibre optique. Si la fibre est étirée ou trop courbée, la présence de minuscules craquelures provoquera la dispersion des rayons lumineux. Une fibre trop coudée peut modifier l'ange incident des rayons lumineux qui entrent en contact avec la limite coeur-enveloppe. Si cet angle devient inférieur à l'angle critique de la réflexion interne totale, certains rayons lumineux seront perdus car ils se réfracteront dans l'enveloppe au lieu de se réfléchir autour de la courbure. [1] [2]

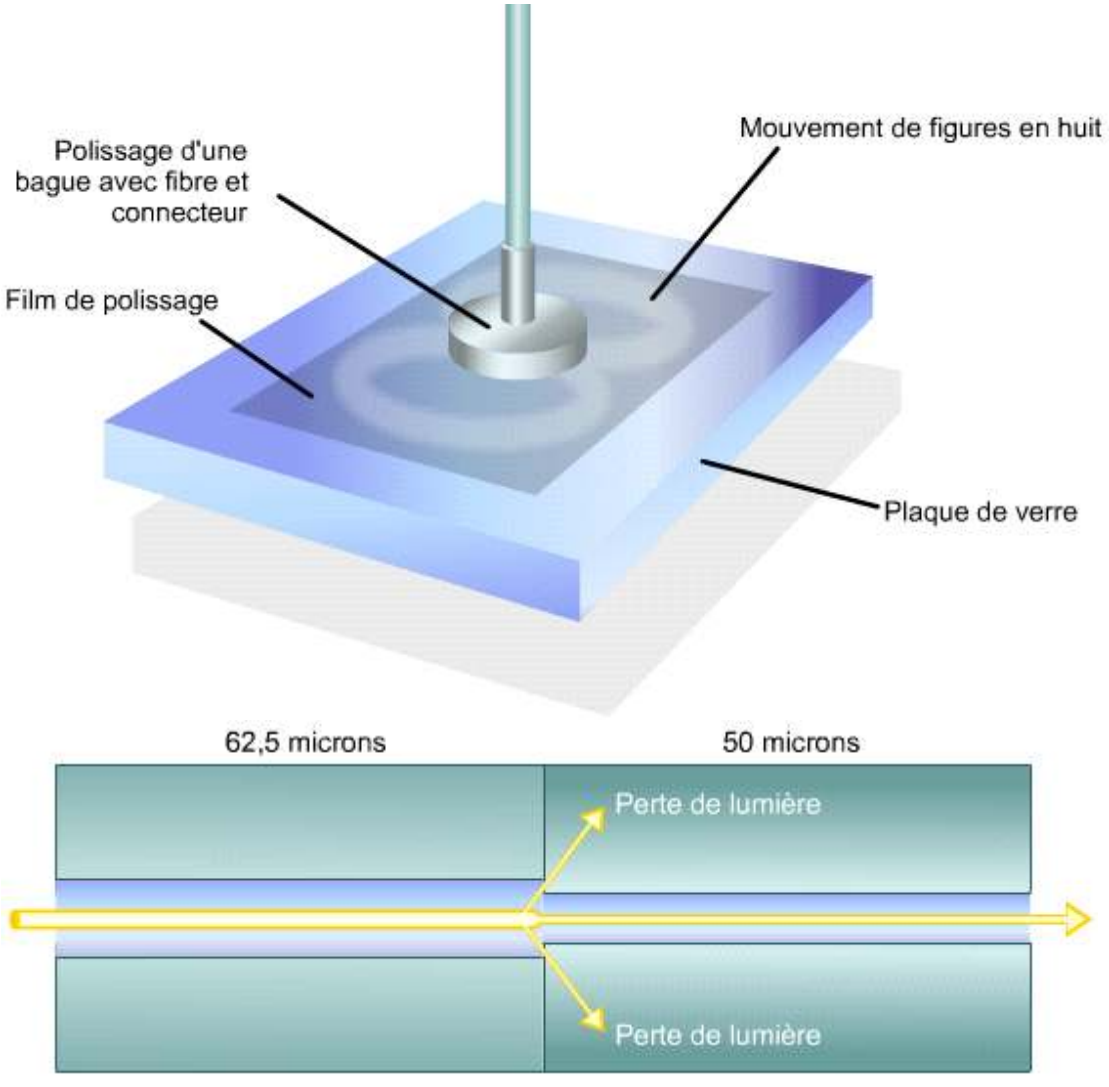


Pour éviter les courbures excessives, la fibre est généralement introduite dans un conduit plus raide que la fibre elle-même et donc, plus difficile à plier. Ce conduit protège également la fibre contre tout étirement lors d'une installation et empêche le dépassement du rayon de courbure (limite de courbure) de la fibre.

Une fois la fibre installée, ses extrémités doivent être coupées avec soin de façon à ce qu'elles soient lisses. [3]


Finition linéaire : Provoque le réfléchissement de la lumière dans la fibre en raison d'un bond dans l'indice de réfraction
Finition linéaire
Intervalle d'air
Angle : Les connecteurs polis entraînent la réflexion hors du cœur, qui se dissipe dans l'enveloppe.
Finition angulaire
Contact des surfaces angulaires
Contact physique : Réduit le réfléchissement en raison de l'infime discontinuité de l'indice de réfraction.
Finition arrondie
Contact physique
Connecteur ultra-poli : Utilise plusieurs couches de film de polissage pour obtenir une surface ultra-lisse.
Finition arrondie ultra-fine
Contact physique

Un microscope ou un appareil de test doté d'une loupe permet d'examiner l'extrémité de la fibre et de vérifier qu'elle est correcte. Un connecteur est ensuite fixé à l'extrémité. Des connecteurs mal installés, des épissures incorrectes ou l'assemblage de deux câbles dont le diamètre du coeur est différent contribuent à réduire considérablement la puissance d'un signal lumineux. [4] [5]



Une fois le câble à fibre optique et les connecteurs correctement installés, vérifiez que ces derniers sont propres. Les extrémités doivent être recouvertes d'un protecteur isolant pour éviter qu'elles se détériorent. Avant de connecter la fibre au port d'un commutateur ou d'un routeur, retirer le protecteur isolant des connecteurs de chaque fibre utilisée et nettoyez l'extrémité de chaque connecteur à l'aide d'un chiffon non pelucheux imbibé d'alcool isopropylique. Les ports de média optique d'un commutateur ou d'un routeur doivent contenir également ce protecteur isolant s'ils ne sont pas utilisés et nettoyés de la même façon avant de les fixer à une fibre optique. Des extrémités sales diminuent considérablement l'intensité de la lumière qui atteint le récepteur.

La dispersion, l'absorption, une installation incorrecte et des extrémités sales dégradent la puissance des signaux lumineux et sont considérées comme une nuisance appelée bruit. Avant d'utiliser un câble à fibre optique, vous devez vérifier que la lumière atteignant réellement le récepteur est suffisante afin que ce dernier puisse détecter les zéros et les uns dans le signal.

Si vous prévoyez d'installer des liaisons par fibre optique, vous devez calculer la perte de puissance de signal tolérée, c'est-à-dire le budget à allouer à l'affaiblissement des liaisons optiques par rapport, par exemple, à un budget mensuel. Une fois toutes les dépenses déduites des recettes initiales, les fonds disponibles doivent être suffisants pour couvrir le mois.

Le décibel (dB) est l'unité de mesure de la perte de puissance. Il indique le pourcentage de puissance sortant de l'émetteur et entrant réellement dans le récepteur.

Il est très important de tester les extrémités d'un câble à fibre optique et d'enregistrer les résultats du test. Il existe divers modèles d'appareil de test de fibre optique. Les deux modèles les plus importants sont les appareils de mesure de perte optique et les réflectomètres *(Optical Time Domain Reflectometer, OTDR)*. 6



Ces deux appareils vérifient que la fibre optique des câbles est conforme aux normes TIA et que la perte de puissance de la liaison n'est pas inférieure au budget alloué à l'affaiblissement des liaisons optiques. Les réflectomètres fournissent des informations de diagnostic supplémentaires sur les liaisons optiques. Ils permettent également de résoudre les problèmes de liaison.

Cette leçon est terminée. La leçon suivante traite des médias sans fil. La première page est consacrée au organismes de normalisation et aux normes régissant les réseaux locaux sans fil.

3.3 Médias sans fil

3.3.1 Organisations de normalisation et normes des LAN sans fil (WLAN)

Cette page présente les réglementations et les normes qui s'appliquent à la technologie sans fil et garantissent que les réseaux déployés sont conformes et interopérables.

À l'instar des réseaux câblés, l'IEEE est le premier éditeur de normes en matière de réseaux sans fil. Ces normes ont été élaborées dans le cadre des réglementations instaurées par la FCC *(Federal Communications Commission)*. 1

- 802.11
- 802.11b
- 802.11a
- 802.11g

Le DSSS *(Direct Sequence Spread Spectrum* ou *étalement du spectre en séquence directe)* est une technologie clé contenue dans la norme 802.11 qui s'applique aux équipements sans fil fonctionnant dans la gamme des 1 à 2 Mbits/s. Un système DSSS pouvant fonctionner jusqu'à un débit de 11 Mbits/s n'est pas considéré comme étant conforme au-dessus des 2 Mbits/s. La norme 802.11b a été ensuite approuvée pour accroître les fonctions de transmission à 11 Mbits/s. Même si les LAN sans fil DSSS pouvaient interopérer avec les LAN sans fil FHSS *(Frequency Hopping Spread Spectrum* ou *étalement du spectre à sauts de fréquence)*, certains problèmes ont conduit les constructeurs à modifier leur conception. Dans ce contexte, l'IEEE a créé une norme qui correspondait à la solution proposée par les constructeurs.

La norme 802.11b est aussi appelée norme Wi-Fi™ ou norme sans fil haut débit pour les systèmes DSSS qui opèrent à 1, 2, 5,5 et 11 Mbits/s. Tous les systèmes 802.11b sont compatibles en amont dans la mesure où ils prennent également en charge la norme 802.11 à 1 et 2 Mbits/s s'appliquant au DSSS uniquement. Cette compatibilité amont est extrêmement importante car elle permet de mettre à niveau le réseau sans fil sans remplacer les cartes réseau ou les points d'accès.

Les équipements 802.11b prennent en charge un débit de données plus élevé en recourant à une technique de codage différente de celle des équipements 802.11, qui les autorise à transmettre une plus grande quantité de données dans le même délai. La plupart des équipements 802.11b ne parviennent toujours pas à atteindre une largeur de bande de 11 Mbits/s et fonctionnent généralement à un débit compris entre 2 et 4 Mbits/s.

La norme 802.11a s'applique aux équipements de réseau LAN sans fil opérant dans la bande de transmission de 5 GHz. La plage de 5 GHz ne permet pas l'interopérabilité des équipements 802.11b lorsqu'ils opèrent à 2,4 GHz. Les équipements 802.11a réalisent un débit de données de 54 Mbits/s et peuvent atteindre 108 Mbits/s grâce à la technologie propriétaire qui permet de doubler le débit. Dans les réseaux de production, la norme se situe plutôt entre 20 et 26 Mbits/s.

Les équipements 802.11g fournissent la même bande passante que les équipements 802.11a, mais avec une compatibilité en amont pour les équipements 802.11b utilisant la technologie de modulation OFDM (*Orthogonal Frequency Division Multiplexing* ou *multiplexage par répartition orthogonale de la fréquence*) et fonctionnent dans la bande de transmission de 2,4 GHz. Cisco a développé un point d'accès qui autorise les équipements 802.11b et 802.11a à coexister sur le même LAN sans fil. Ce point d'accès fournit des services de passerelle permettant à ces équipements normalement incompatibles de communiquer entre eux.

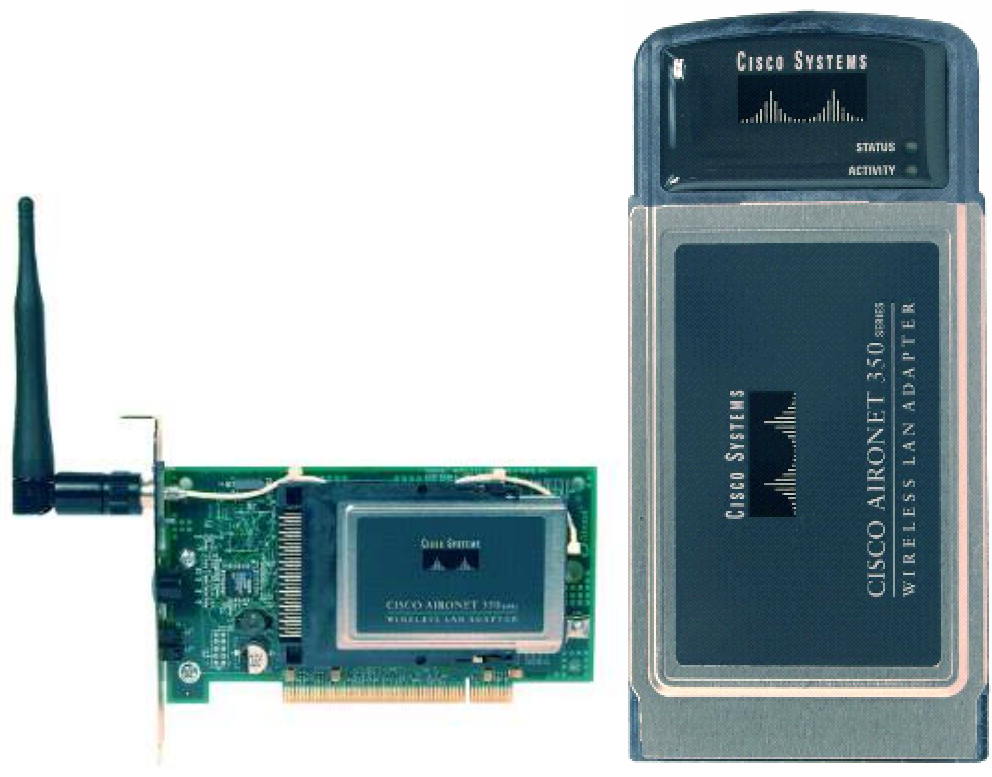
La page suivante décrit les topologies et les équipements utilisés dans les réseaux sans fil.

3.3 Médias sans fil

3.3.2 Équipements et topologies sans fil

Cette page décrit les équipements et les topologies d'un réseau sans fil.

Il suffit de deux équipements pour créer un réseau sans fil. 1 – 3

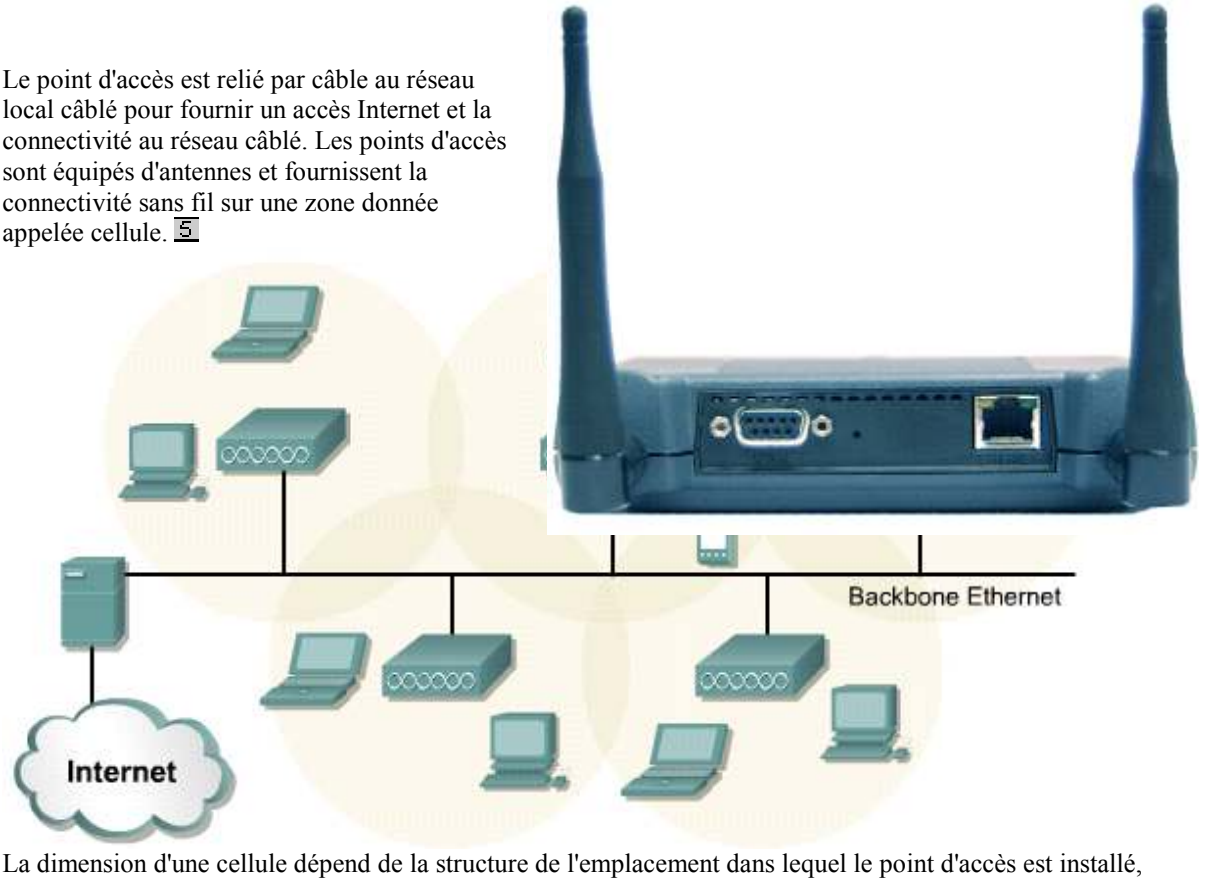




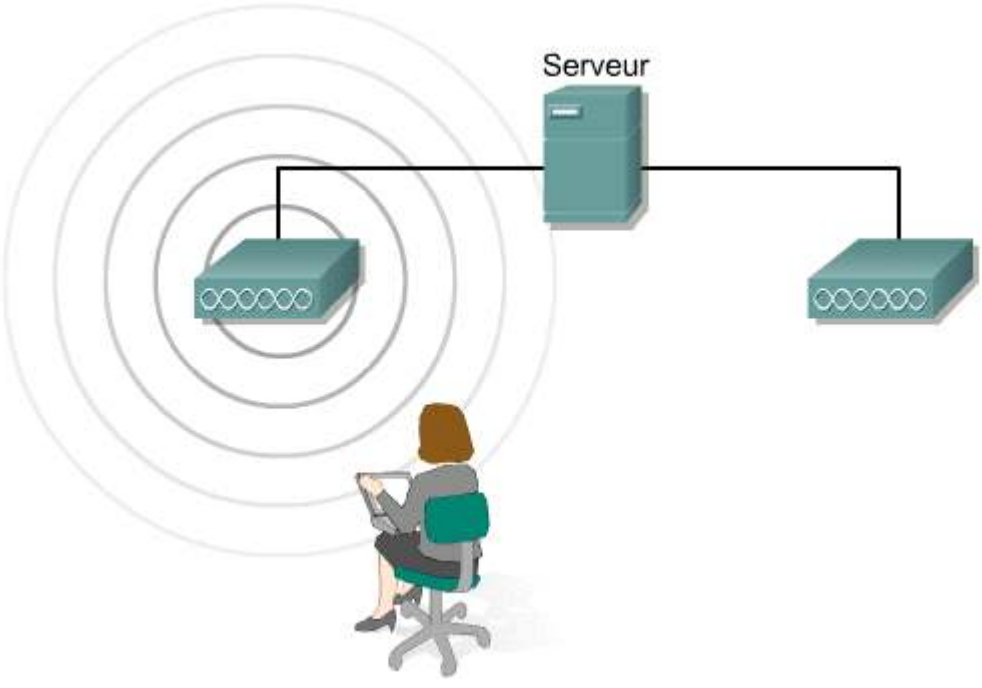
Un nœud peut être tout simplement un ordinateur de bureau ou un ordinateur portable. Il est possible de créer un réseau sur mesure (ad hoc) avec des cartes réseau sans fil, comparable à un réseau câblé d'égal à égal. Les deux équipements se comportent comme des serveurs et des clients dans cet environnement. Bien que la connectivité soit assurée, ce type de réseau fournit un niveau de sécurité et un débit médiocres. De plus, il ne résout pas le problème d'incompatibilité dû au fait que des cartes réseau de constructeurs différents sont souvent incompatibles.

Pour résoudre le problème d'incompatibilité, un point d'accès est généralement installé pour servir de concentrateur central dans le mode infrastructure des LAN sans fil. 4

Le point d'accès est relié par câble au réseau local câblé pour fournir un accès Internet et la connectivité au réseau câblé. Les points d'accès sont équipés d'antennes et fournissent la connectivité sans fil sur une zone donnée appelée cellule. 5



La dimension d'une cellule dépend de la structure de l'emplacement dans lequel le point d'accès est installé, outre la taille et la puissance des antennes. Elle est généralement comprise entre 91,44 et 152,4 mètres. Pour desservir des zones plus vastes, il est possible d'installer plusieurs points d'accès avec un degré de chevauchement permettant le «roaming» entre les cellules. 6



Ce processus est très similaire aux services fournis par les opérateurs de téléphonie cellulaire. Dans de nombreux réseaux de points d'accès, le chevauchement est important pour permettre le déplacement des équipements au sein du LAN sans fil. Un chevauchement de 20 à 30 % est souhaitable, bien que les normes IEEE ne le spécifient pas. Comme ce pourcentage favorise le «roaming» entre les cellules, l'activité de déconnexion et de reconnexion peut se produire en toute transparence sans interruption de service.

Lorsqu'un client est activé au sein du LAN sans fil, il commence par écouter un équipement compatible auquel il est «associé». Cette «exploration» peut être active ou passive.

L'exploration active entraîne l'envoi d'une demande de sonde de la part du nœud sans fil cherchant à joindre le réseau. Cette demande contient l'identifiant de l'ensemble de services (SSID) du réseau qu'il souhaite joindre. Si un point d'accès ayant le même SSID est trouvé, il émet une réponse de sonde et les étapes d'authentification et d'association sont terminées.

Le nœuds d'exploration passive écoutent les trames de gestion Beacon qui sont transmises par le point d'accès (mode infrastructure) ou les nœuds d'égal à égal (mode ad hoc). Lorsqu'un nœud reçoit une trame Beacon contenant le SSID du réseau qu'il cherche à joindre, une tentative d'accès au réseau est effectuée. L'exploration passive est un processus continu où les nœuds peuvent s'associer aux points d'accès ou s'en dissocier dès que la puissance du signal varie.

La première activité de média interactive indique les niveaux du modèle de référence OSI et les équipements réseau associés.

La seconde activité de média interactive illustre l'addition d'un concentrateur sans fil à un réseau câblé. La page suivante explique comment communiquent les réseaux LAN sans fil.

Activité de média interactive

Interactivité: Équipements des couches OSI

Cette animation classe les équipements réseau selon la couche OSI au niveau de laquelle ils opèrent.

Activité de média interactive

Pointer-cliquer: Du réseau local câblé au réseau local sans fil

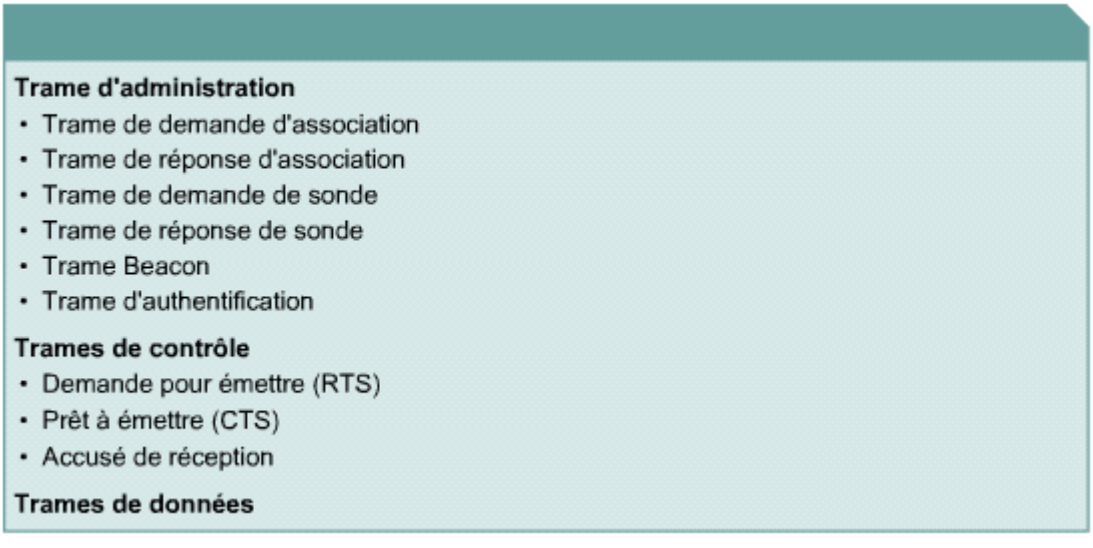
Cette activité illustre un réseau local câblé classique.

3.3 Médias sans fil

3.3.3 Mode de communication des réseaux LAN sans fil

Cette page explique le processus de communication d'un LAN sans fil.

Après avoir établi la connectivité à un LAN sans fil, un nœud transmet les trames de la même manière que dans n'importe quel réseau 802.x. Comme les LAN sans fil n'utilisent pas la trame 802.3 standard, l'expression «Ethernet sans fil» prête à confusion. Il existe trois types de trame : les trames de contrôle, d'administration et de données. [1]


Trame d'administration
• Trame de demande d'association
• Trame de réponse d'association
• Trame de demande de sonde
• Trame de réponse de sonde
• Trame Beacon
• Trame d'authentification
Trames de contrôle
• Demande pour émettre (RTS)
• Prêt à émettre (CTS)
• Accusé de réception
Trames de données

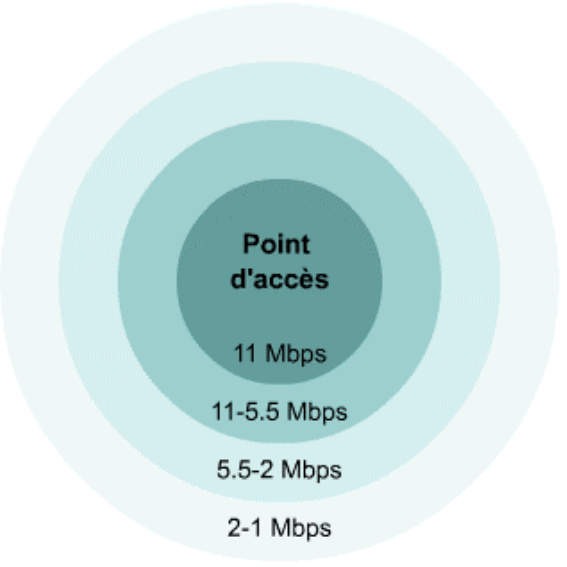
Seules les trames de données sont similaires aux trames 802.3. Les trames sans fil et 802.3 comportent 1 500 octets de données utiles. Cependant, une trame Ethernet ne peut dépasser 1518 octets alors qu'une trame sans fil peut atteindre 2 346 octets. En général, la trame d'un LAN sans fil est limitée à 1 518 octets, car elle est connectée la plupart du temps à un réseau Ethernet câblé.

Étant donné que la radiofréquence (RF) est un média partagé, il peut se produire des collisions comme dans tout autre média partagé, à la différence près qu'il n'existe aucune méthode permettant au nœud source de détecter les collisions. C'est la raison pour laquelle les LAN sans fil utilisent la détection de porteuse avec accès multiple et prévention de collision (CSMA/CA), similaire au réseau CSMA/CD Ethernet.

Lorsqu'un nœud source envoie une trame, le nœud récepteur renvoie un accusé de réception positif, ce qui consomme 50 % de la bande passante disponible. Cette charge, combinée à celle du protocole de prévention de collision, réduit le débit de données réel à un débit maximal compris entre 5 et 5,5 Mbits/s sur un LAN sans fil 802.11b de 11 Mbits/s.

Les performances du réseau sont également affectées par la puissance du signal et une dégradation de la qualité du signal due à la distance ou aux interférences. Comme le signal devient plus faible, la sélection de débit adaptable peut être invoquée. Le débit de l'unité émettrice diminue en passant de 11 Mbit/s à 5,5 Mbits/s, de 5,5 Mbits/s à 2 Mbits/s ou de 2 Mbits/ à 1 Mbits/s. [2]

La page suivante explique l'authentification et l'association.



3.3 Médias sans fil
3.3.4 Authentification et association

Cette page décrit l'authentification et l'association dans le cadre des réseaux LAN sans fil.

L'authentification des LAN sans fil a lieu au niveau de la couche 2. Il s'agit du processus d'authentification d'un équipement et non de l'utilisateur. Ce processus est important dans le contexte de la sécurité, de la résolution des problèmes et de l'administration globale des LAN sans fil.

L'authentification peut être un processus nul, comme dans le cas d'un nouveau point d'accès et d'une nouvelle carte réseau avec des configurations par défaut en place. Le client envoie au point d'accès une trame de demande d'authentification, et le point d'accès accepte ou refuse la trame. Le client est averti de la réponse via une trame de réponse d'authentification. Le point d'accès peut également être configuré de façon à confier la tâche d'authentification à un serveur d'authentification qui pourrait réaliser un processus plus crédible. 1



L'association effectuée après l'authentification est l'état qui permet à un client d'utiliser les services du point d'accès pour transmettre des données.

Types d'authentification et d'association

- Non authentifié et non associé
  - Le nœud est déconnecté du réseau et non associé à un point d'accès.
- Authentifié et non associé
  - Le nœud a été authentifié sur le réseau mais n'est pas encore associé au point d'accès.
- Authentifié et associé
  - Le nœud est connecté au réseau et peut transmettre et recevoir des données via le point d'accès.

Méthodes d'authentification
La norme IEEE 802.11 spécifie deux types de processus d'authentification.

Le premier est le système ouvert (open). Il s'agit d'une norme de connectivité standard dans laquelle seul le SSID doit correspondre. Cette norme peut être utilisée dans un environnement sécurisé ou non, bien qu'il soit fort probable que des sniffeurs de réseau de niveau inférieur découvrent le SSID du réseau LAN sans fil.

Le second processus est la clé partagée (shared key). Ce processus requiert l'utilisation du cryptage WEP (*Wired Equivalent Privacy*), un algorithme simple utilisant des clés de 64 et 128 bits. Le point d'accès est configuré avec une clé cryptée, et les nœuds tentant d'accéder au réseau via le point d'accès doivent disposer d'une clé correspondante. Les clés WEP attribuées de façon statique fournissent un niveau de sécurité supérieur à celui du système ouvert, mais elles ne sont pas inviolables.

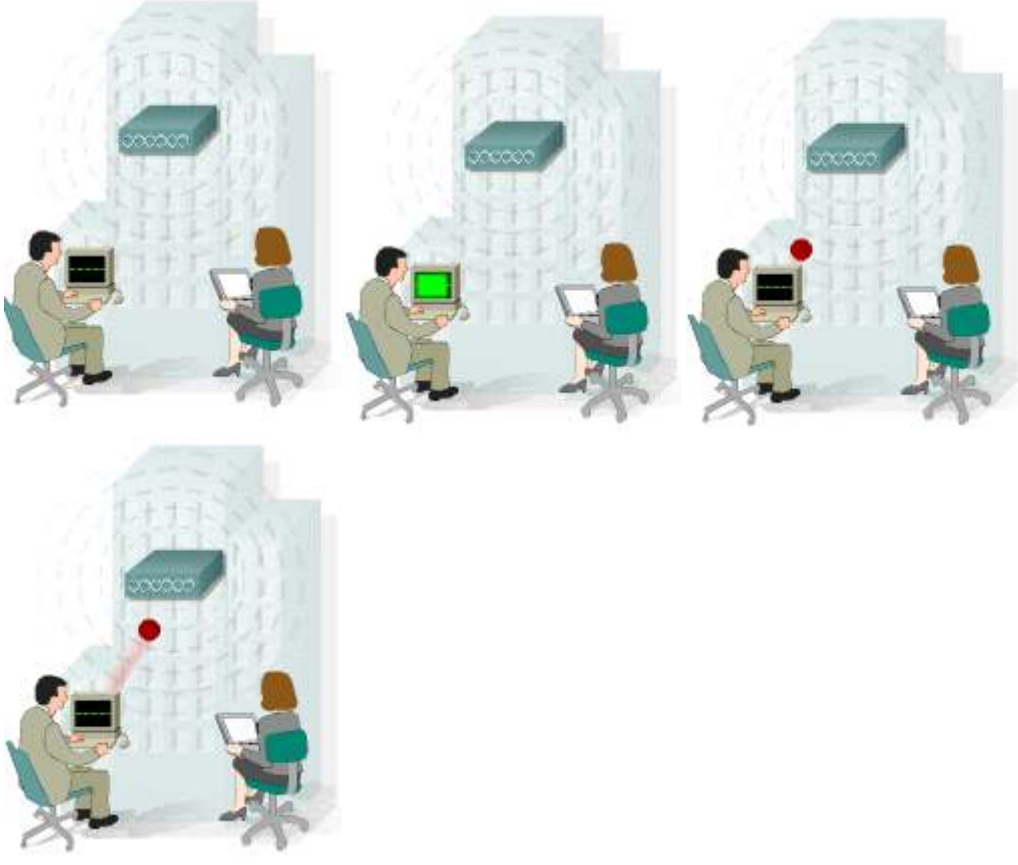
Le problème d'une entrée non autorisée dans un LAN sans fil est traité par un grand nombre de nouvelles technologies de solution de sécurité.

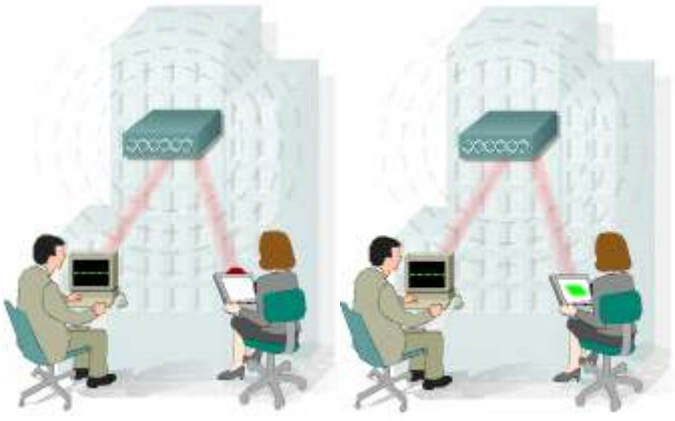
La page suivante décrit les ondes radioélectriques et la modulation.

3.3 Médias sans fil
3.3.5 Spectres des ondes radioélectrique et des micro-ondes

Cette page décrit les ondes radioélectriques et la modulation.

Les ordinateurs envoient des signaux de données par voie électronique et les émetteurs radio convertissent ces signaux électriques en ondes radioélectriques. La variation des courants électriques dans l'antenne d'un émetteur génère des ondes radioélectriques qui se propagent sous forme de lignes droites à partir de l'antenne. 1





Toutefois, les ondes radioélectriques s'atténuent lorsqu'elles sortent de l'antenne émettrice. Dans un LAN sans fil, la puissance d'un signal radio mesuré à une distance de 10 mètres de l'antenne émettrice serait égale à un centième de sa puissance d'origine. À l'instar de la lumière, les ondes radioélectriques peuvent être absorbées par certains matériaux et réfléchies par d'autres. Lors du passage d'une matière telle que l'air à une autre matière telle qu'un mur en plâtre, les ondes radioélectriques sont réfractées. Elles sont également dispersées et absorbées par les gouttelettes d'eau présentes dans l'air.

Il est important de retenir ces qualités des ondes radioélectriques lors de la planification d'un réseau LAN sans fil destiné à un immeuble ou à un campus. L'étude de site désigne le processus d'évaluation d'un emplacement pour l'installation d'un LAN sans fil.

Comme les signaux radio s'affaiblissent lorsqu'ils circulent hors de l'émetteur, le récepteur doit aussi être équipé d'une antenne. Lorsque des ondes radioélectriques entrent en contact avec l'antenne d'un récepteur, des courants électriques de faible intensité sont générés dans cette antenne. Ces courants électriques générés par les ondes radioélectriques reçues sont égaux aux courants qui ont généré initialement les ondes radioélectriques dans l'antenne de l'émetteur. Le récepteur amplifie la puissance de ces signaux électriques affaiblis. 2







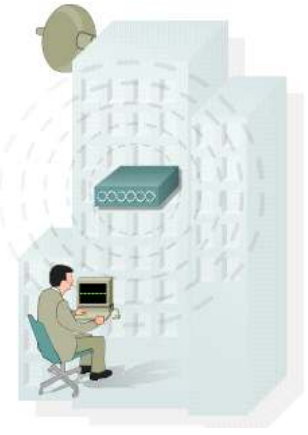










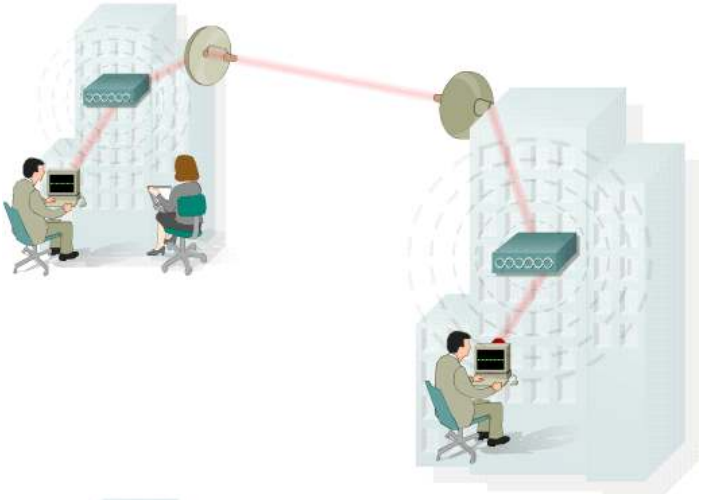


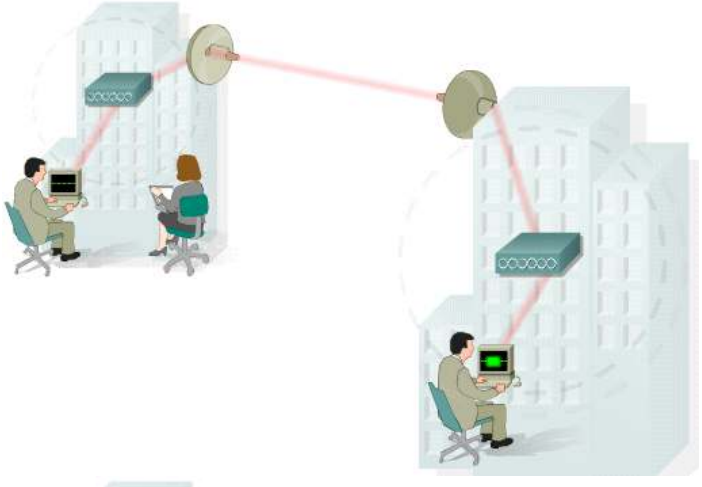


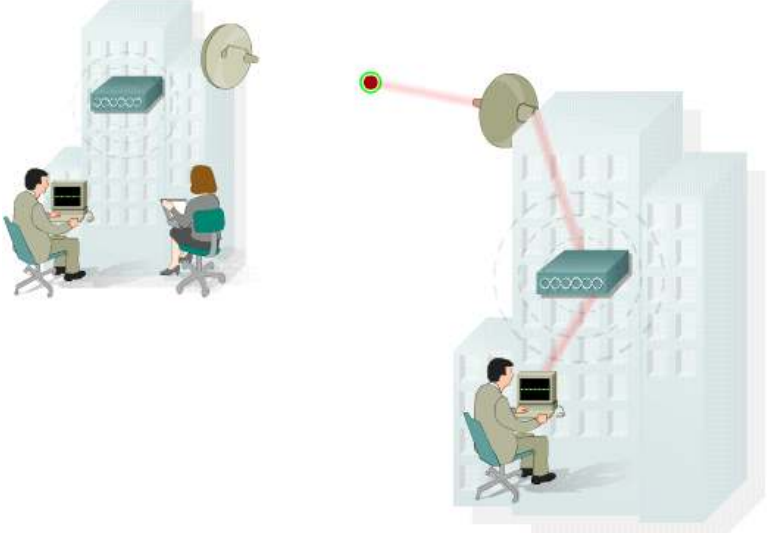


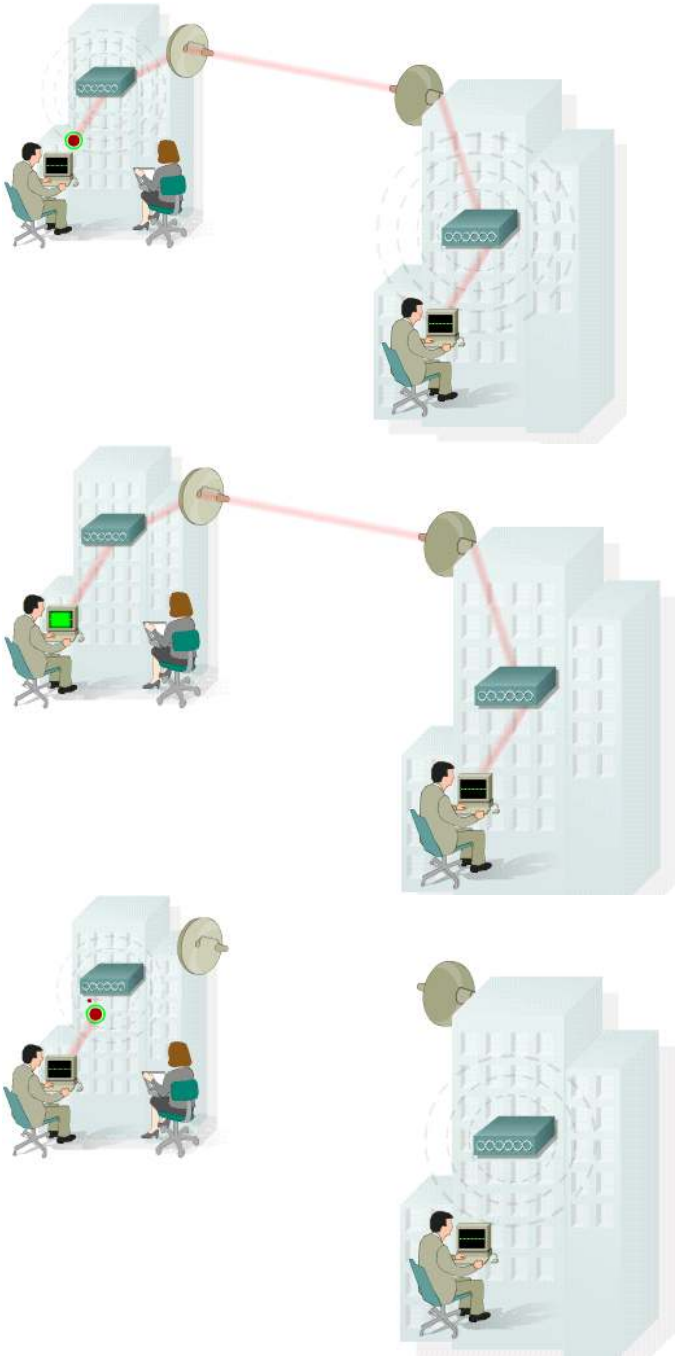


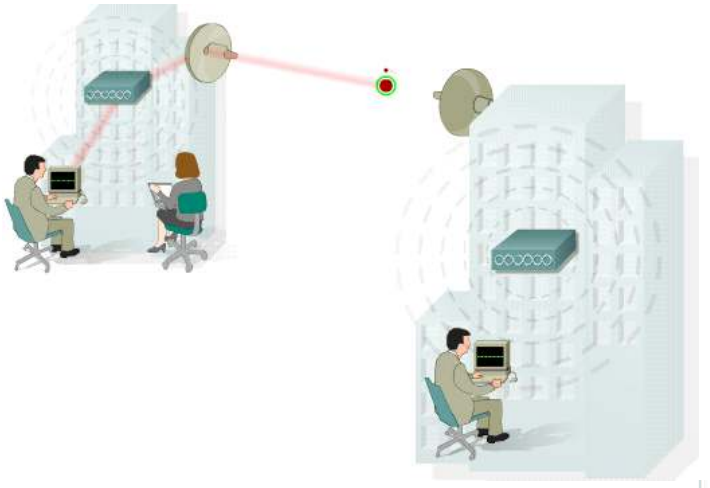


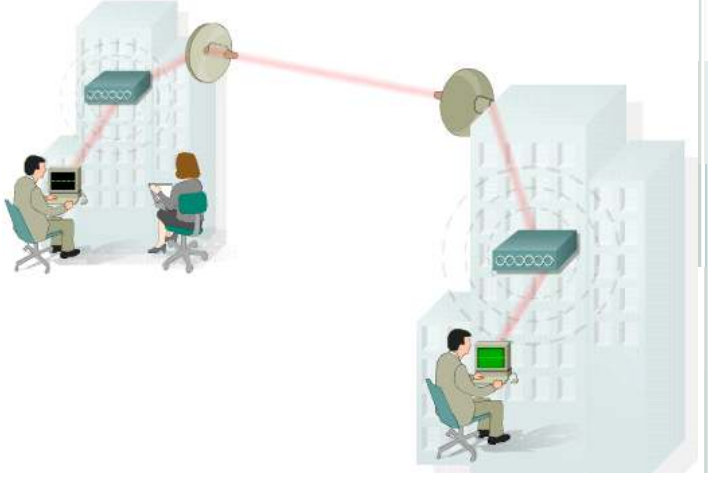








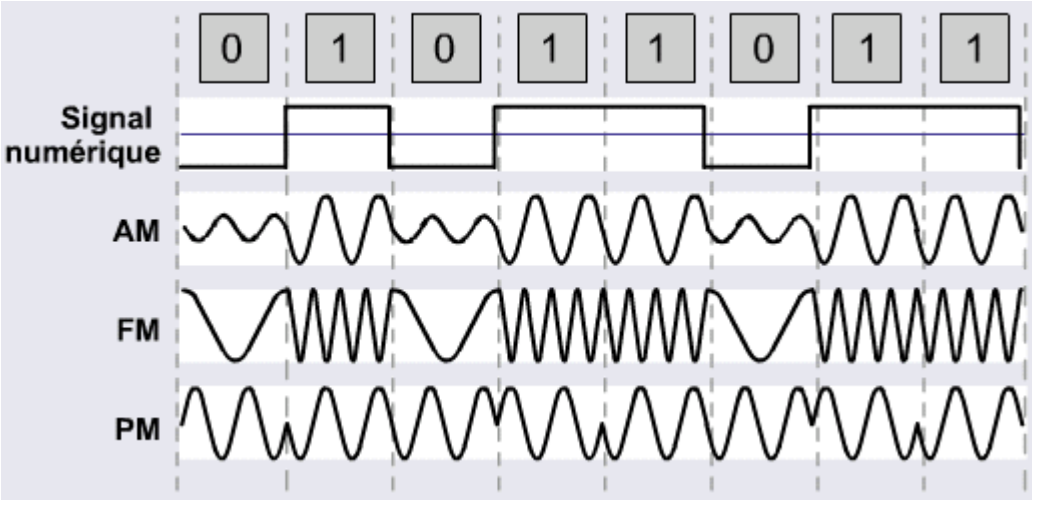






Dans un émetteur, les signaux (de données) électriques en provenance d'un ordinateur ou d'un réseau local ne sont pas envoyés directement à l'antenne de l'émetteur, mais sont utilisés pour modifier un second signal puissant appelé signal porteur.

Le processus de modification du signal porteur entrant dans l'antenne de l'émetteur est appelé modulation. Un signal porteur radioélectrique peut être modulé dans trois cas principaux. Par exemple, les stations de radio à modulation d'amplitude (AM) modulent la hauteur (amplitude) du signal porteur. Les stations de radio à modulation de fréquence (FM) modulent la fréquence du signal porteur, tel que déterminé par le signal électrique du micro. Dans les LAN sans fil, un troisième type de modulation appelé modulation de phase permet de superposer le signal de données sur le signal porteur diffusé par l'émetteur. 3



Dans ce type de modulation, les bits de données du signal électrique modifient la phase du signal porteur.

Un récepteur démodule le signal porteur en provenance de son antenne. Il interprète les modifications de phase du signal porteur et le reconstitue à partir du signal de données électrique d'origine.

La première activité de média interactive explique les champs électromagnétiques et la polarisation.

La seconde activité de média interactive indique les noms, les équipements, les fréquences et les longueurs d'onde du spectre électromagnétique.

La page suivante décrit les problèmes liés aux signaux et au bruit.

Activité de média interactive

Pointer-cliquer: Champs électromagnétiques et polarisation

Cette activité comprend une série de graphiques animés qui illustrent les champs électromagnétiques et la polarisation.

Activité de média interactive

Interactivité: Spectre électromagnétique

Cette activité permet de faire défiler le spectre électromagnétique en déplaçant la souris vers la gauche ou la droite du graphique.

3.3 Médias sans fil

3.3.6 Signaux et bruit dans les réseaux LAN sans fil

Cette page décrit la façon dont les signaux et le bruit peuvent affecter un réseau LAN sans fil.

Dans un réseau Ethernet câblé, il est généralement simple de diagnostiquer la cause des interférences. La technologie RF (radiofréquence) permet de prendre en compte divers types d'interférence.

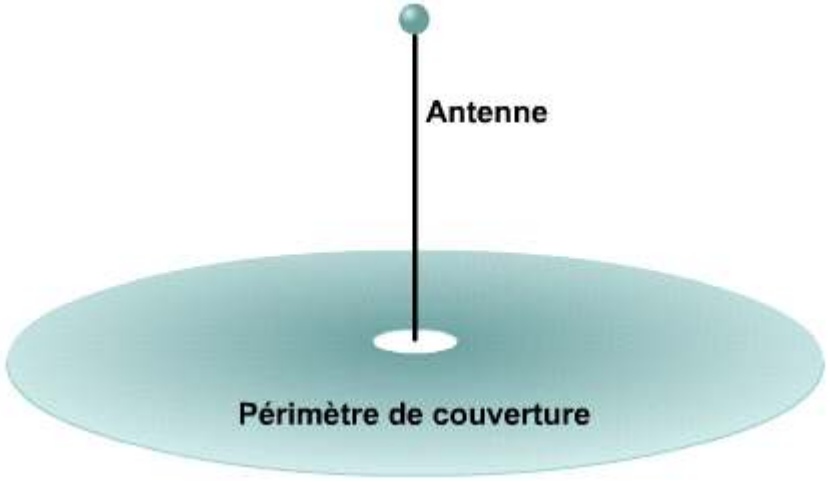
La technologie à bande étroite est l'inverse de la technologie de l'étalement du spectre. Comme son nom l'indique, la technologie à bande étroite n'affecte pas l'intégralité du spectre de fréquences du signal sans fil. Pour résoudre un problème d'interférence à bande étroite, il suffirait de modifier le canal utilisé par le point d'accès. En réalité, la recherche de la cause d'une interférence à bande étroite peut prendre du temps et s'avérer coûteuse. L'identification de la source requiert un analyseur de spectre dont le modèle le plus économique est relativement onéreux.

Une interférence de bande entière affecte l'intégralité du spectre. La technologie Bluetooth™ franchit plusieurs fois 2,4 GHz par seconde et peut engendrer d'importantes interférences sur un réseau 802.11b. Il n'est pas rare de voir dans les lieux utilisant des réseaux sans fil des écriteaux demandant l'arrêt de tous les équipements Bluetooth™ avant d'entrer. Dans les habitations et les bureaux, les interférences proviennent souvent des fours à micro-ondes. Il suffit d'une fuite d'une micro-onde d'un watt dans le spectre RF pour entraîner une panne de réseau importante. Les téléphones sans fil opérant dans le spectre de 2,4 GHz peuvent également perturber un réseau.

En règle générale, les conditions météorologiques les plus extrêmes ne peuvent pas affecter un signal RF. Cependant, le brouillard ou des conditions d'humidité extrêmes peuvent perturber les réseaux sans fil. La foudre peut également charger l'atmosphère et modifier le parcours d'un signal transmis.

La première origine évidente d'un problème de signal est la station émettrice et le type d'antenne. Une station à haut rendement transmet le signal et une antenne parabolique concentrant le signal augmente la plage de transmission.

Dans les petits bureaux, la plupart des points d'accès utilisent des antennes jumelles équidirectives pour transmettre le signal dans toutes les directions, ce qui réduit la portée de communication. 1



La page suivante décrit la sécurité des réseaux LAN sans fil.

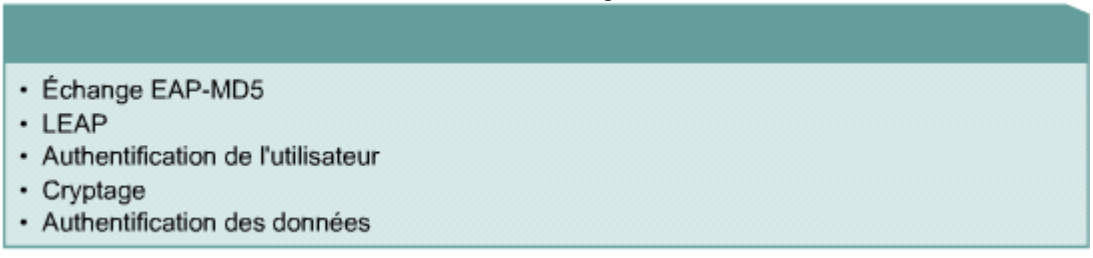
3.3 Médias sans fil

3.3.7 Sécurité des réseaux LAN sans fil

Cette page explique comment mettre en oeuvre la sécurité sur les réseaux LAN sans fil.

Le manque de sécurité a toujours été un inconvénient pour les réseaux sans fil, depuis leur apparition. Aujourd'hui, de nombreux administrateurs ne savent pas encore mettre en oeuvre des mesures de sécurité efficaces.

Un grand nombre de nouveaux protocoles et solutions de sécurité tels que les réseaux privés virtuels (VPN) et le protocole EAP *(Extensible Authentication Protocol)* sont désormais disponibles. Avec le protocole EAP, le point d'accès ne fournit plus l'authentification au client, mais transmet les tâches à un équipement plus perfectionné, par exemple à un serveur réservé à cet effet. Une technologie VPN de serveur intégrée crée un tunnel au début d'un protocole existant tel que le protocole IP. Il s'agit d'une connexion de couche 3, contrairement à la connexion de couche 2 située entre le point d'accès et le nœud émetteur. 1



- **EAP-MD5 Challenge** – Le protocole EAP *(Extensible Authentication Protocol)* est le type d'authentification le plus ancien, très proche de la protection par mot de passe CHAP sur un réseau câblé.
- **LEAP (Cisco)** – Le protocole LEAP *(Lightweight Extensible Authentication Protocol)* est le type d'authentification principalement utilisé dans les points d'accès des LAN sans fil Cisco. Ce protocole assure la sécurité pendant les échanges des autorisations, utilise des clés WEP de cryptage dynamique et prend en charge l'authentification mutuelle.
- **Authentification utilisateur** – Permet uniquement aux utilisateurs autorisés à se connecter et à envoyer et à recevoir des données sur le réseau sans fil.
- **Cryptage** – Fournit des services de cryptage qui protègent les données des intrus.
- **Authentification des données** – Assure l'intégrité des données en authentifiant les équipements d'origine et de destination.

La technologie VPN ferme efficacement le réseau sans fil, car un LAN sans fil non limité envoie automatiquement le trafic entre les nœuds qui apparaissent comme étant situés sur le même réseau sans fil. Comme les réseaux sans fil s'étendent souvent hors du périmètre de l'habitation ou du bureau dans lesquels ils sont installés, des intrus peuvent facilement s'y infiltrer. En contrepartie, un administrateur réseau peut mettre en oeuvre rapidement une sécurité minimale sur un LAN sans fil.

Cette leçon est terminée. La page suivante récapitule les principaux points évoqués au cours de ce module.

Résumé

Cette page récapitule les thèmes abordés tout au long du module.

Les câbles de cuivre transportent les informations via le courant électrique. Les caractéristiques électriques d'un câble déterminent le type de signal pouvant être transmis par le câble, ainsi que la vitesse de transmission du signal et la distance que peut parcourir ce dernier.

La compréhension des concepts électriques suivants est utile pour intervenir dans les réseaux informatiques:

- **Tension** – Pression qui déplace les électrons d'un emplacement à un autre dans un circuit.
- **Résistance** – Opposition au flux d'électrons et raison pour laquelle un signal se dégrade lorsqu'il se déplace dans un conduit.
- **Courant** – Flux des charges créées lors d'un déplacement d'électrons.
- **Circuits** – Boucle fermée dans laquelle circule un courant électrique.

Les circuits doivent être composés de matériaux conducteurs et posséder des sources de tension. La tension entraîne la circulation du courant, alors que la résistance et l'impédance s'y opposent. Un multimètre sert à mesurer numériquement la tension, le courant, la résistance et d'autres quantités électriques.

Les câbles coaxiaux, les câbles à paires torsadées non blindées et les câbles à paires torsadées blindées sont des types de câble qui peuvent être utilisés dans un réseau pour assurer différentes fonctions. Un câble à paires torsadées peut être un câble droit, un câble croisé ou un câble console (à paires inversées). Ces termes désignent les connexions de chaque fil, ou configurations, d'une extrémité à l'autre du câble. Un câble droit sert à relier deux équipements différents tels qu'un commutateur et un PC. Un câble croisé permet de relier deux équipements similaires tels que deux PC. Un câble à paires inversées permet de connecter un PC au port console d'un routeur. Différentes connexions sont nécessaires car l'emplacement des broches de transmission et de réception est différent sur chacun de ces équipements.

La fibre optique est le média le plus couramment utilisé pour assurer les transmissions point-à-point, plus longues et à haut débit sur des backbones de réseau local (LAN) et sur des réseaux longue distance (WAN). L'énergie lumineuse permet de transmettre en toute sécurité de grandes quantités de données sur des distances relativement longues. Le signal lumineux transporté par une fibre est produit par un émetteur qui convertit les signaux électriques en signaux lumineux. Le récepteur reconvertit la lumière provenant de l'extrémité du câble en signal électrique d'origine.

Chaque câble à fibre optique utilisé dans les réseaux comprend deux fibres de verre logées dans des enveloppes distinctes. Les circuits à fibre optique utilisent un brin de fibre pour transmettre et un brin de fibre pour recevoir, comme un câble de cuivre à paires torsadées utilise des paires de fils individuelles pour transmettre et recevoir.

Le coeur d'une fibre optique est la partie à travers laquelle circulent les rayons lumineux. L'enveloppe qui entoure le coeur réfléchit le signal vers le coeur. La gaine intermédiaire entourant l'enveloppe protège celle-ci et le coeur contre tout dommage. Le matériau de résistance entourant la gaine intermédiaire empêche le câble de fibre de s'étirer au cours des installations. Il s'agit souvent du Kevlar. Le dernier élément, la gaine externe, enveloppe le câble pour protéger la fibre contre l'abrasion, les solvants et autres contaminants.

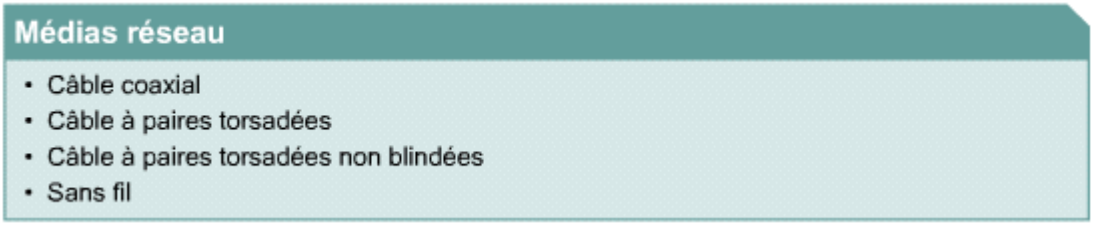
Les lois de réflexion et de réfraction permettent de concevoir une fibre guidant les ondes lumineuses qui la traversent avec un minimum de perte d'énergie et de signal. Une fois au coeur de la fibre, un rayon lumineux ne peut suivre qu'un nombre limité de chemins optiques. Ces chemins sont appelés modes. Si le diamètre du coeur de la fibre est suffisamment large de façon à ce que la lumière puisse suivre plusieurs chemins à l'intérieur de la fibre, celle-ci est appelée fibre multimode. En revanche, les rayons lumineux ne disposent que d'un seul mode pour circuler au coeur d'une fibre monomode dont le diamètre est plus petit. En raison de sa conception, la fibre monomode prend en charge des débits de données plus élevés et des distances plus longues que la fibre multimode.

La fibre est considérée comme insensible au bruit, car elle n'est pas perturbée par le bruit externe ou le bruit provenant des autres câbles. La lumière confinée dans une fibre ne peut en aucun cas s'infiltrer dans une autre fibre. L'atténuation d'un signal sonore constitue un problème sur de longs câbles, particulièrement si des sections du câble sont épissées ou connectées à des panneaux de brassage.

Avec des médias de cuivre et à fibre optique, les équipements ne peuvent être déplacés que dans les limites des médias auxquels ils sont connectés. La technologie sans fil supprime ces contraintes. Les réglementations et normes s'appliquant à la technologie sans fil garantissent que les réseaux déployés seront interopérables et conformes aux normes IEEE 802.11 des réseaux LAN sans fil.

Il suffit de deux équipements pour créer un réseau sans fil. L'équivalent sans fil d'un réseau d'égal à égal auquel sont connectés directement les équipements de l'utilisateur final est une topologie sans fil ad hoc. Pour résoudre les problèmes d'incompatibilité entre les équipements, une topologie en mode infrastructure peut être mise en oeuvre à l'aide d'un point d'accès qui se comporte comme un concentrateur central au sein du LAN sans fil. La communication sans fil utilise trois type de trame : les trames de contrôle, d'administration et de données. Pour éviter les collisions sur les média de radiofréquence partagés, les LAN sans fil utilisent la détection de porteuse avec accès multiple et prévention de collision (CSMA/CA).

L'authentification des réseaux LAN sans fil est un processus de couche 2 qui authentifie l'équipement, et non l'utilisateur. L'association effectuée après l'authentification permet à un client d'utiliser les services du point d'accès pour transmettre des données.



4-Teste des cables

Vue d'ensemble

Les médias réseau constituent littéralement et physiquement la colonne vertébrale d'un réseau. Un câblage réseau de qualité médiocre entraîne des défaillances du réseau et de mauvaises performances. Il est nécessaire de tester les médias réseau en cuivre, à fibre optique ou sans fil afin de s'assurer qu'ils répondent à des exigences strictes. Ces tests impliquent de connaître certains concepts électriques et mathématiques ainsi que des termes comme signal, onde, fréquence et bruit. Ces termes aideront les étudiants à comprendre le fonctionnement des réseaux, des câbles et des tests des câbles.

La première partie de ce module propose des définitions de base pour permettre aux étudiants de mieux appréhender les notions de test des câbles présentées dans la deuxième partie.

La deuxième partie décrit les problèmes liés au test des câbles pour la connectivité de la couche physique dans les LAN. Afin que le LAN fonctionne correctement, le média de la couche physique doit être conforme aux normes de l'industrie.

L'atténuation (affaiblissement d'un signal) et le bruit (signal parasite) peuvent poser des problèmes sur les réseaux car les données envoyées sont susceptibles d'être mal interprétées ou de ne pas être reconnues après réception. Il est important que la terminaison des connecteurs de câbles et l'installation des câbles soient correctement effectuées. Si les normes sont respectées durant l'installation, les réparations et les remplacements, les niveaux d'atténuation et de bruit peuvent être réduits.

Après l'installation d'un câble, un testeur de certification peut vérifier que les installations répondent bien aux normes TIA/EIA. Ce module décrit également le déroulement de tests importants.

Il traite, par ailleurs, certains objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811. [2] [3]

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Mise en œuvre d'un LAN	• Dépannage d'un LAN simple	

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Description des propriétés et des normes physiques, électriques et mécaniques relatives aux médias optiques, sans fil et en cuivr utilisés pour les réseaux. • Description des problème physiques et de topologie associés au câblage des LAN les plus courants

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes: [1]

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
4.1	Notions de base pour étudier les tests de câbles basés sur la réponse en fréquences
4.2	Signaux et bruit

- Distinguer les ondes sinusoïdales des ondes carrées
- Définir et calculer des exposants et des logarithmes
- Définir et calculer des décibels
- Définir des termes de base relatifs au temps, à la fréquence et au bruit
- Faire la distinction entre une bande passante numérique et une bande passante analogique
- Comparer les niveaux de bruit sur différents types de câbles
- Définir et décrire les effets d'une atténuation et d'un défaut d'adaptation de l'impédance
- Montrer comment les paires torsadées peuvent réduire le bruit
- Montrer comment la diaphonie et les paires torsadées peuvent réduire le bruit
- Décrire les dix tests des câbles en cuivre spécifiés dans la norme TIA/EIA-568-B
- Décrire les différences entre les câbles de catégorie 5 et les câbles de catégorie 6

4.1 Test des câbles basé sur la fréquence

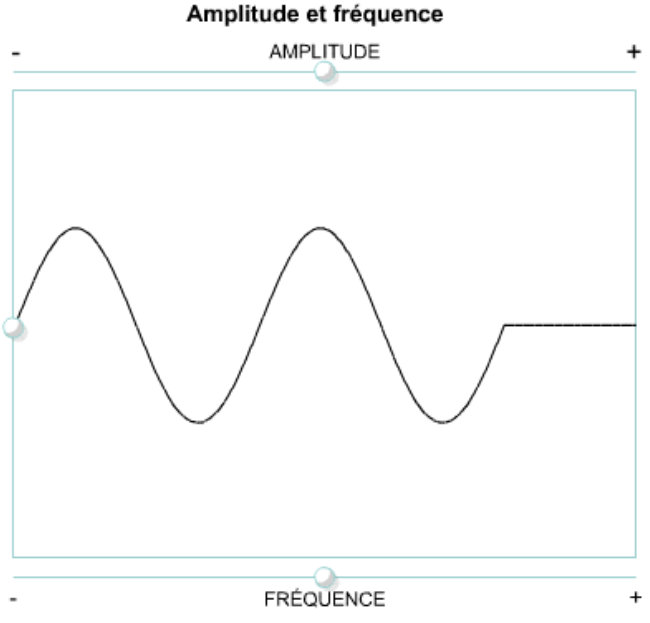
4.1.1 Ondes

Cette première partie fournit des définitions relatives au test des câbles basé sur la fréquence. Cette page traite des ondes.

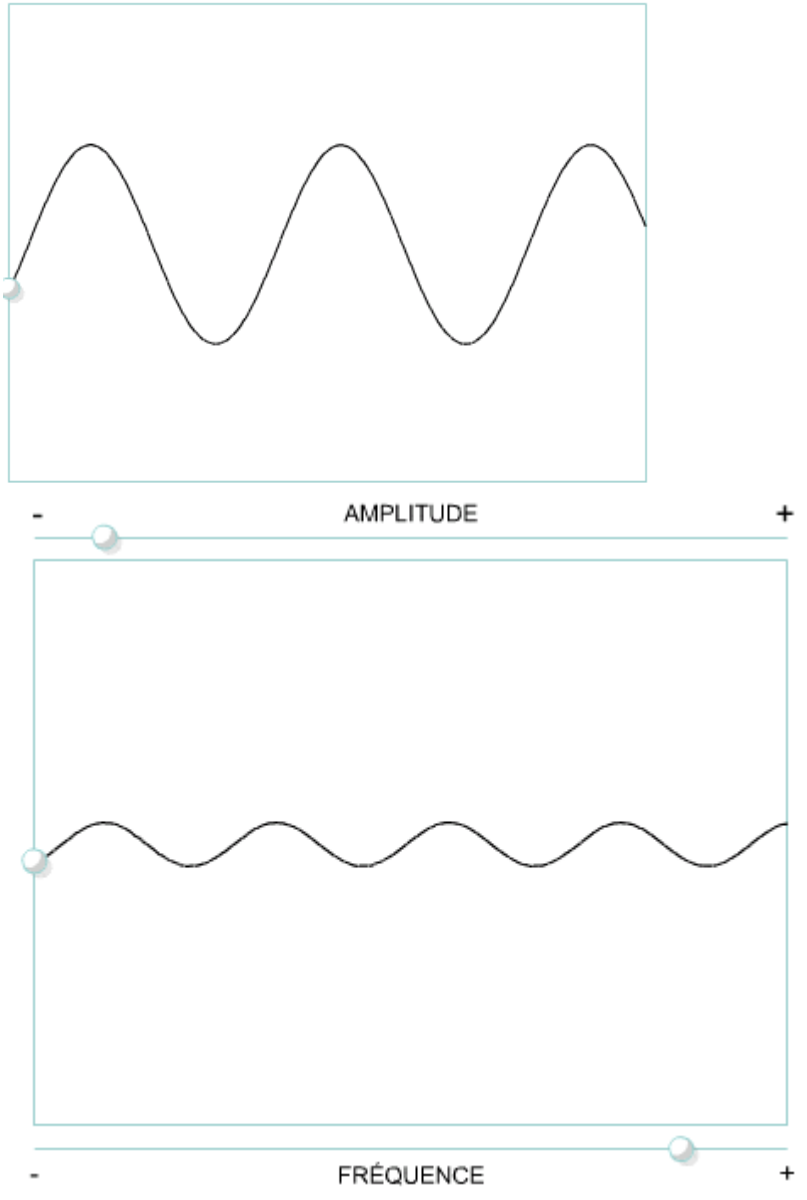
Une onde est de l'énergie qui circule d'un endroit à l'autre. Il existe de nombreuses sortes d'ondes, mais toutes peuvent être décrites avec le même vocabulaire.

Les ondes peuvent être comparées à des perturbations. Un seau dont l'eau est complètement immobile ne contient pas d'ondes puisqu'il ne subit pas de perturbations. Par contre, l'océan qui subit l'influence du vent et des marées présente en permanence des ondes détectables, aussi réduites soient-elles.

Les vagues de l'océan, comparables à des ondes, se définissent par leur hauteur, c'est-à-dire leur amplitude, mesurée en mètres. Elles peuvent également se définir selon la fréquence avec laquelle elles atteignent le rivage, à savoir leur période et leur fréquence. La période correspond à l'intervalle entre deux vagues (exprimé en secondes). La fréquence correspond au nombre de vagues qui atteignent le rivage chaque seconde. Elle se mesure en hertz (Hz). 1 Hz équivaut à 1 onde par seconde, soit 1 cycle par seconde. Afin de vous familiariser avec ces concepts, ajustez l'amplitude et la fréquence sur la figure 1



Ajustez l'amplitude et la fréquence de l'onde sinusoïdale



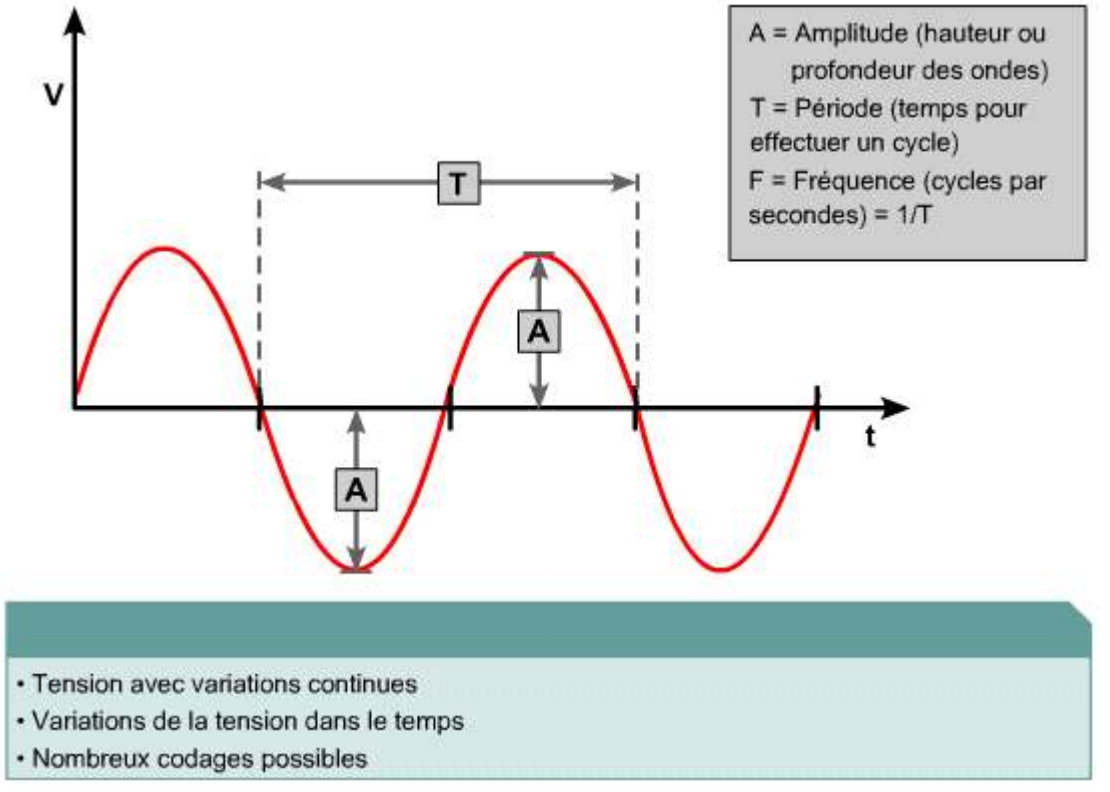
Les spécialistes des réseaux s'intéressent plus particulièrement aux ondes de tension dans les médias en cuivre, aux ondes lumineuses dans les fibres optiques ainsi qu'aux champs électriques et électromagnétiques ou ondes électromagnétiques. L'amplitude d'un signal électrique correspond toujours à la hauteur de l'onde mais se mesure en volts (V) et non en mètres (m). La période est le temps que met 1 cycle à se dérouler. Elle se mesure en secondes. La fréquence est le nombre de cycles complets par seconde. Elle se mesure en hertz.

Une perturbation provoquée délibérément et impliquant une durée fixe et prévisible est appelée impulsion. Les impulsions jouent un rôle important dans les signaux électriques. En effet, elles constituent la base de la transmission numérique. La forme de ces impulsions représente la valeur des données transmises.

La page suivante est une introduction aux ondes sinusoïdales et carrées.

Cette page aborde la notion d'onde sinusoïdale et d'onde carrée.

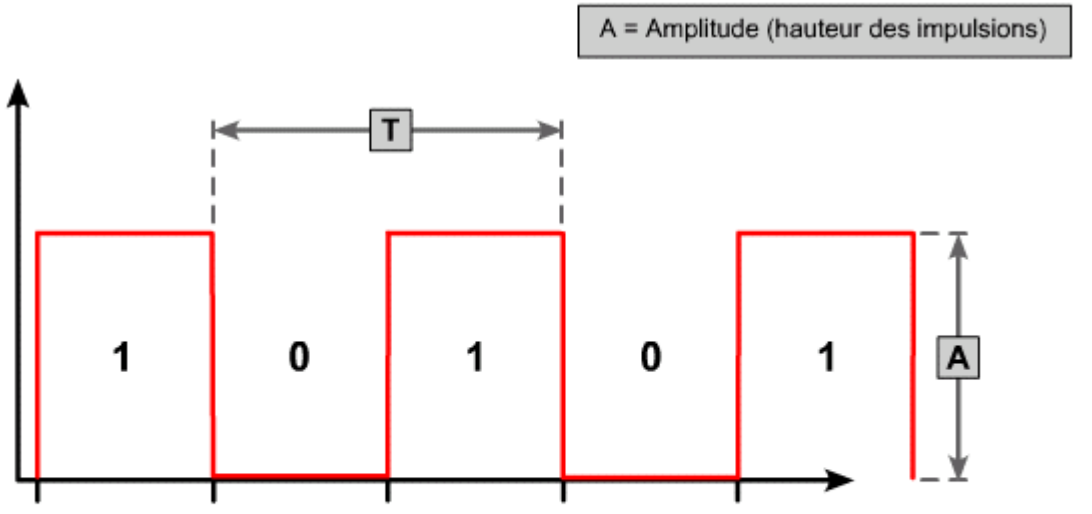
Les ondes sinusoïdales, ou sinusoïdes, sont des représentations de fonctions mathématiques. [1]


A = Amplitude (hauteur ou profondeur des ondes)
T = Période (temps pour effectuer un cycle)
F = Fréquence (cycles par secondes) = 1/T
V
T
A
A
t
• Tension avec variations continues
• Variations de la tension dans le temps
• Nombreux codages possibles

Elles sont périodiques, c'est-à-dire qu'elles répètent le même schéma de courbe à intervalles réguliers. En outre, elles varient continuellement, ce qui signifie qu'aucun point n'a la même valeur que celui qui le précède ou le suit immédiatement sur le graphique.

Elles sont des représentations graphiques d'événements qui se répètent naturellement et changent à intervalles de temps réguliers. C'est le cas de la distance entre la Terre et le Soleil, de la distance entre le sol et celui qui se trouve sur une grande roue, ou encore de l'heure à laquelle le jour se lève. Les ondes sinusoïdales variant en permanence, elles constituent un exemple d'ondes analogiques.

Tout comme les ondes sinusoïdales, les ondes carrées sont périodiques. [2]



- Impulsions discrètes (non continues)
- Seulement deux états possibles (1/0, allumé/éteint)
- Sauts de tension entre les niveaux

Cependant, les graphiques des ondes carrées ne varient pas avec le temps. L'onde garde la même valeur, puis se modifie brusquement. Après quelques courts instants, elle reprend sa valeur de départ. Les ondes carrées sont des signaux numériques, ou impulsions. À l'image de toutes les ondes, elles se caractérisent par leur amplitude, leur période et leur fréquence.

La page suivante traite des exposants et des logarithmes.

4.1 Test des câbles basé sur la fréquence

4.1.3 Exposants et logarithmes

Cette page explique les notions d'exposant et de logarithme.

Il existe trois systèmes de numération dans les réseaux: 1

Il existe trois systèmes de numération dans les réseaux :
- Base 2 : binaire
- Base 10 : décimal
- Base 16 : hexadécimal

- **Le système binaire** (à base 2)
- **Le système décimal** (à base 10)
- **Le système hexadécimal** (à base 16)

Rappelez-vous que la base d'un système de numération correspond au nombre de symboles différents qui peuvent occuper une position. Par exemple, les nombres binaires n'ont que deux valeurs possibles : 0 et 1. Les

nombres décimaux ont dix valeurs différentes possibles, de 0 à 9, tandis que les nombres hexadécimaux en ont 16 : les nombres de 0 à 9 et les lettres de A à F.

Notez que 10 x 10 peut s'écrire 10^2. 10^2 signifie 10 au carré ou encore 10 puissance 2. 10 correspond à la base du nombre et 2 à son exposant. 10 x 10 x 10 peut s'écrire 10^3. 10^3 signifie 10 au cube ou encore 10 puissance 3. La base du nombre est 10 et son exposant est 3. Utilisez l'activité de média interactive pour calculer des exposants. Saisissez une valeur de x pour calculer y ou une valeur de y pour calculer x.

La base d'un système de numération correspond également à la valeur de chaque chiffre. Le plus petit chiffre a une valeur de base^0, soit 1. Le chiffre immédiatement supérieur a une valeur de base^1, ce qui équivaut à 2 pour les nombres binaires, 10 pour les nombres décimaux et 16 pour les hexadécimaux.

Les nombres avec exposants sont utilisés pour représenter de façon aisée des nombres très grands ou très petits. Représenter numériquement un milliard par 10^9 est beaucoup plus facile et entraîne bien moins d'erreurs que d'écrire 1 000 000 000. De nombreux calculs liés aux tests de câblage font intervenir des nombres très grands qui imposent l'utilisation d'exposants. Utilisez l'activité de média interactive pour élargir vos connaissances sur les exposants.

Une autre manière de manipuler les nombres très grands et très petits est de transformer les nombres à partir de règles mathématiques appelées logarithmes. La forme abrégée de logarithme est « log ». Tout nombre peut servir de base à un système de logarithmes. Cependant, la base 10 présente de nombreux avantages pour les calculs ordinaires, contrairement à d'autres bases. La base 10 est d'ailleurs presque exclusivement utilisée pour des calculs ordinaires. Les logarithmes dont la base est 10 sont appelés logarithmes décimaux. Il est impossible d'obtenir le logarithme d'un nombre négatif.

Afin de calculer le logarithme d'un nombre, servez-vous d'une calculatrice ou de l'activité de média interactive. Par exemple, log (10^9) = 9. Il est possible de calculer le logarithme de nombres qui ne sont pas des puissances de 10. Il n'est pas possible de calculer le logarithme d'un nombre négatif. L'étude des logarithmes n'est pas au programme de ce cours. Toutefois, leur terminologie est souvent utilisée pour calculer des décibels et mesurer l'intensité d'un signal sur des médias en cuivre, à fibre optique ou sans fil.

La page suivante explique la façon dont sont mesurés les décibels.



Activité de média interactive

Interactivité: Logarithmes

Cette activité calcule des logarithmes de base 10 selon les valeurs entrées pour x et y.



Activité de média interactive

Interactivité: Puissances de 10

Cette activité permet de calculer des puissances de 10.

4.1 Test des câbles basé sur la fréquence

4.1.4 Décibels

Cette page présente un aperçu de ce que sont les décibels.

Le décibel (dB) est une unité de mesure utilisée pour décrire des signaux réseau. Son calcul fait appel aux exposants et aux logarithmes décrits précédemment. Deux formules servent à calculer les décibels: 1

$dB = 10 \log_{10}(P_{final} / P_{réf})$

$dB = 20 \log_{10} (V_{final} / V_{réf})$

Dans ces formules de calcul, dB représente la perte ou le gain de puissance d'une onde. Les décibels peuvent être des valeurs négatives, ce qui correspond à une perte de puissance dans la propagation d'une onde, ou des valeurs positives, ce qui correspond à un gain de puissance, c'est-à-dire à une amplification du signal.

La variable $\log_{10}$ indique que le nombre entre parenthèses est modifié selon la règle logarithmique décimale.

P_{final} correspond à la puissance de sortie mesurée en watts.

$P_{réf}$ correspond à la puissance d'entrée mesurée en watts.

V_{final} correspond à la tension de sortie mesurée en volts.

$V_{réf}$ correspond à la tension d'entrée mesurée en volts.

La première formule calcule les décibels en termes de puissance (P) et la seconde en termes de tension (V). La première formule est souvent utilisée pour mesurer les ondes lumineuses dans les fibres optiques ainsi que les ondes radioélectriques dans l'air, tandis que la seconde est utilisée pour mesurer les ondes électromagnétiques dans les câbles de cuivre. Ces formules ont plusieurs points communs.

Dans la formule $dB = 10 \log_{10} (P_{final} / P_{réf})$, saisissez des valeurs pour dB et $P_{réf}$ afin de trouver la puissance de sortie. 1

Il existe deux formules pour calculer les décibels :

- $dB = 10 \log_{10} (P_{final}/P_{ref})$
- $dB = 20 \log_{10} (V_{final}/V_{ref})$

Cette formule pourrait permettre de connaître la puissance restante d'une onde radioélectrique ayant traversé les différents matériaux et les différentes étapes de systèmes électroniques tels que les radios. Essayez d'effectuer les exercices suivants avec les activités de média interactives:

- Si la puissance d'entrée de la source laser, ou $P_{réf}$, est de 7 microwatts (1×10^{-6} watts) et que la perte totale d'une liaison à fibre optique est de 13 dB, quelle est la puissance de sortie?
- Si la perte totale d'une liaison à fibre optique est de 84 dB et que la puissance d'entrée de la source laser, ou $P_{réf}$, est de 1 milliwatt, quelle est la puissance de sortie?

- Si 2 microvolts, soit 2 x 10^{-6} volts, sont mesurés à la sortie d'un câble et que la tension d'entrée était d'1 volt, quel est le gain – ou la perte – en décibels? Cette valeur est-elle positive ou négative? S'agit-il d'un gain ou d'une perte de tension?

La page suivante explique comment analyser et visualiser des signaux grâce à un oscilloscope.

Activité de média interactive

Interactivité: Calculs de Décibels

Cette activité permet à l'étudiant de saisir la tension de sortie et la tension d'entrée afin d'obtenir le gain en décibels.

Activité de média interactive

Interactivité: Utilisation des décibels

Cette activité permet à l'étudiant de saisir une valeur pour les décibels et une valeur pour la puissance d'entrée afin d'obtenir la puissance de sortie.

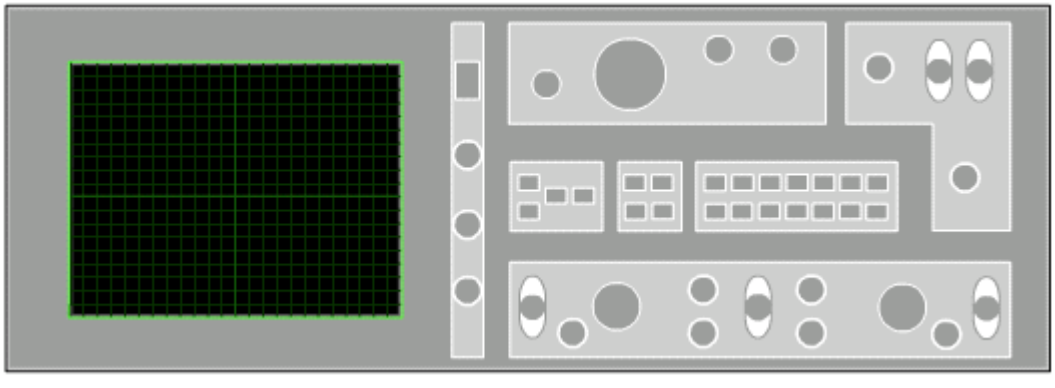
4.1 Test des câbles basé sur la fréquence

4.1.5 Temps et fréquence des signaux

Cette page montre aux étudiants comment analyser et visualiser des signaux.

L'un des traits les plus importants de l'ère informatique est que les caractères, les mots, les images, les vidéos ou la musique sont représentés de manière électrique par des variations de tension dans des câbles ou autres équipements électroniques. Les données que ces variations de tension représentent peuvent être converties en ondes lumineuses ou radioélectriques, puis à nouveau en ondes de tension. Prenez l'exemple d'un téléphone analogique. Les ondes sonores émises par celui qui appelle passent à travers un micro incorporé dans le téléphone. Le micro convertit les variations de l'énergie acoustique en variations d'énergie électrique représentant la voix.

Si la tension est représentée dans le temps par un graphique, les variations de la voix apparaissent à l'écran. 1



Un oscilloscope est un équipement électronique permettant de visualiser des signaux électriques tels que des ondes de tension et des impulsions. Sur l'écran, l'axe des abscisses correspond au temps et l'axe des ordonnées

à la tension ou au courant électrique. Il y a habituellement deux entrées sur l'axe des ordonnées pour permettre d'observer et de mesurer deux signaux simultanément.

L'analyse des signaux à l'aide d'un oscilloscope s'appelle une analyse dans le domaine temporel. L'axe des abscisses, ou domaine de la fonction mathématique, représente le temps. Pour étudier des signaux, les techniciens utilisent également l'analyse dans le domaine de fréquence. Pour cette analyse, l'axe des abscisses représente la fréquence. Un équipement électronique, appelé analyseur de spectre, permet de créer des graphiques pour l'analyse dans le domaine de fréquence. Les signaux électromagnétiques utilisent des fréquences différentes pour la transmission afin que des signaux différents n'interfèrent pas les uns avec les autres. Les signaux radioélectriques à modulation de fréquence (FM) utilisent ainsi des fréquences distinctes de celles de la télévision ou des satellites. Lorsque les auditeurs changent de station de radio, ils changent la fréquence reçue par la radio.

La page suivante traite des variations des signaux réseau.

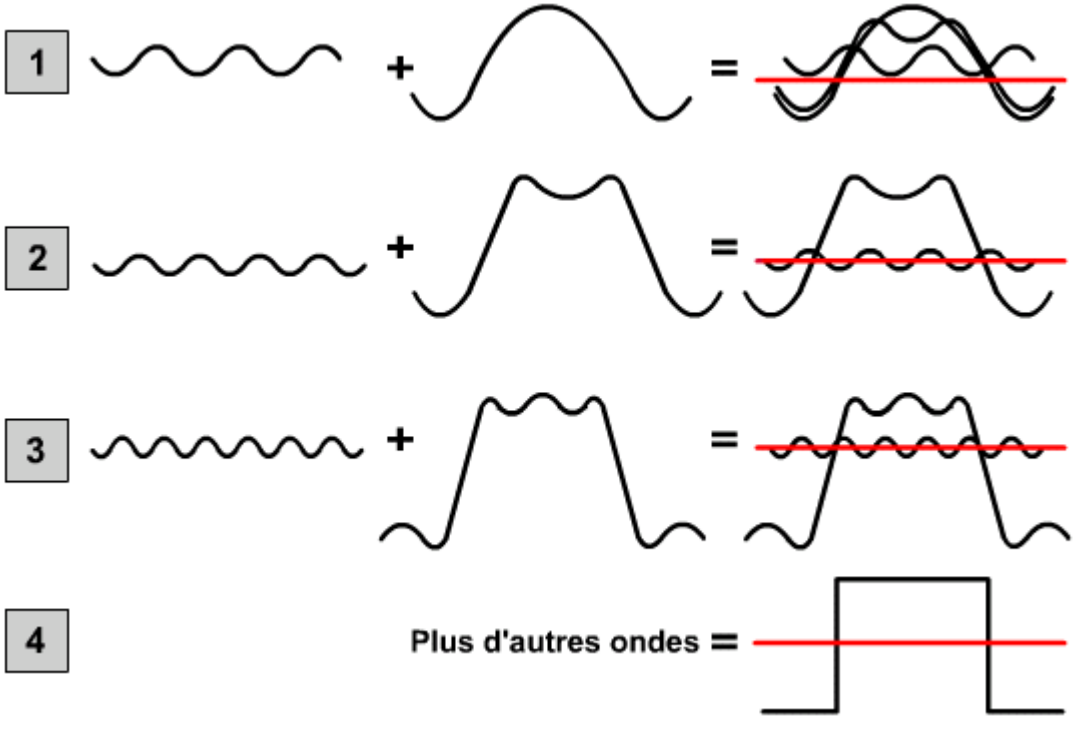
4.1 Test des câbles basé sur la fréquence

4.1.6 Signaux analogiques et numériques

Cette page explique comment les signaux analogiques varient avec le temps et la fréquence.

Tout d'abord, considérons une onde électrique sinusoïdale à fréquence unique pouvant être perçue par l'oreille humaine. Si ce signal est transmis à un haut-parleur, il est possible d'entendre un signal sonore.

Imaginez ensuite une combinaison de plusieurs ondes sinusoïdales. 1



L'onde créée est alors plus complexe qu'une onde sinusoïdale simple. Cette onde comprend plusieurs signaux sonores. Un graphique de ces signaux sonores comprend plusieurs lignes correspondant à la fréquence de chacun d'entre eux.

Pour finir, imaginez un signal complexe tel qu'une voix ou un instrument de musique. Si plusieurs signaux sonores différents sont émis, le graphique montre un spectre continu de signaux sonores individuels.

L'activité de média interactive trace des courbes sinusoïdales et complexes selon l'amplitude, la fréquence et la phase.
La page suivante traite de la notion de bruit.

Activité de média interactive

Interactivité: Synthèse de Fourier

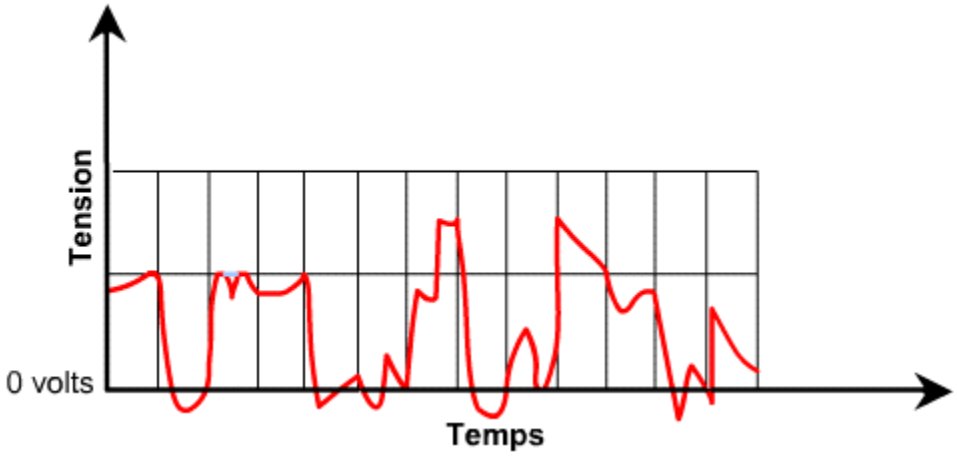
Dans cette activité, l'étudiant trace des ondes sinusoïdales en sélectionnant l'amplitude, la fréquence et la phase pour chacune de ces ondes.

4.1 Test des câbles basé sur la fréquence

4.1.7 Bruit dans le temps et la fréquence

Cette page explique les sources et les effets du bruit.

Le bruit est un concept important dans les réseaux tels que les LAN. 1



La notion de bruit fait généralement référence aux sons. Toutefois, dans les réseaux, il s'agit de signaux parasites. Le bruit peut provenir de sources naturelles ou technologiques, et vient s'ajouter aux signaux de données des systèmes de communication.

Tout système de communication implique une certaine quantité de bruit. Bien que le bruit ne puisse pas être totalement éliminé, ses effets peuvent être réduits grâce à une bonne connaissance de ses sources. Les sources de bruit sont très nombreuses :

- Câbles proches acheminant des signaux de données
- Interférences radioélectriques provenant de signaux tiers proches
- Interférences électromagnétiques provenant d'une source proche telle qu'un moteur ou une ampoule électrique
- Bruit de laser à l'émission ou la réception d'un signal optique

Un bruit qui affecte toutes les fréquences de transmission de la même façon est appelé un bruit blanc. Le bruit n'affectant qu'une petite gamme de fréquences est appelé interférence à bande étroite. Un bruit blanc sur un récepteur radio interfère avec toutes les stations de radio, tandis que l'interférence à bande étroite n'affecte que

quelques stations dont les fréquences sont très proches. Un bruit blanc affectera donc toutes les transmissions de données d'un LAN, une interférence à bande étroite ne perturbant, quant à elle, que certains signaux.

L'activité de média interactive permet aux étudiants de provoquer un bruit blanc et une interférence à bande étroite.

La page suivante traite de bande passante analogique et de bande passante numérique.



Activité de média interactive

Interactivité: Bruit blanc et bruit à bande étroite

Cette activité permet à l'étudiant de saisir une valeur pour l'amplitude et pour la fréquence afin d'obtenir un bruit blanc et un bruit à bande étroite.

4.1 Test des câbles basé sur la fréquence

4.1.8 Bande passante

Cette page porte sur le concept de bande passante, très important dans le domaine des réseaux.

Deux sortes de bandes passantes sont importantes pour l'étude d'un LAN : la bande passante analogique et la bande passante numérique.

La bande passante analogique fait référence à la plage de fréquences d'un système électronique analogique. La bande passante analogique permet de décrire la plage de fréquences émises par une station de radio ou un amplificateur électronique. Comme pour la fréquence, l'unité de mesure de la bande passante analogique est le hertz (Hz).

La bande passante numérique mesure la quantité de données pouvant circuler d'un endroit à un autre pendant une période donnée. 1

Unité de bande passante	Abréviation	Équivalences
Bits par seconde	bits/s	1 kbit/s = 1 000 bits/s
Kilobits par seconde	kbits/s	1 kbit/s = 1 000 bits/s
Mégabits par seconde	Mbits/s	1 Mbit/s = 1 000 000 bits/s = 1 000 kbits/s
Gigabits par seconde	Gbits/s	1 Gbit/s = 1 000 000 000 bits/s = 1 000 Mbits/s

L'unité de mesure de base pour la bande passante numérique est le nombre de bits par seconde (bits/s). Sur les LAN, les vitesses de transmission atteignant des milliers, voire des millions de bits par seconde, elles sont exprimées en kilobits par seconde (Kbits/s) ou mégabits par seconde (Mbits/s). La bande passante est limitée par les médias physiques, les technologies actuelles ainsi que les lois de la physique.

Lors d'un test de câble en cuivre, la bande passante analogique sert à déterminer la bande passante numérique. Les ondes numériques sont constituées de plusieurs ondes sinusoïdales (ondes analogiques). Les fréquences analogiques sont émises à une extrémité et reçues à l'autre extrémité du câble. Les deux signaux sont ensuite comparés et le niveau d'atténuation du signal est calculé. En général, les médias supportant des bandes passantes analogiques importantes sans trop d'atténuation supportent également des bandes passantes numériques élevées.

Cette leçon est terminée. La page suivante traite des signaux et du bruit. Nous allons tout d'abord décrire les câbles en cuivre et à fibre optique.

4.2 Signaux et bruits

4.2.1 Signaux transitant par des câbles en cuivre et à fibre optique

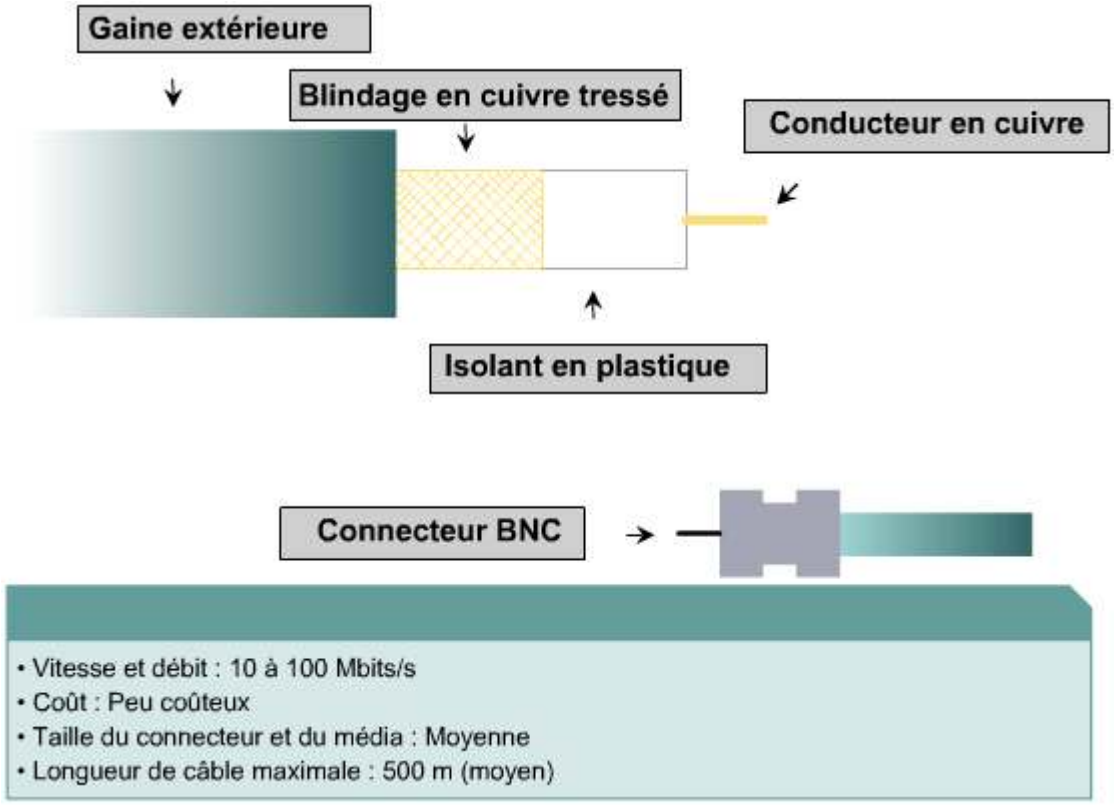
Cette page traite des signaux qui transitent par des câbles en cuivre et à fibre optique.

Dans les câbles en cuivre, les signaux de données correspondent à des niveaux de tension représentés de façon binaire par des 1 et des 0. Les niveaux de tension sont mesurés pour l'émetteur et le récepteur à partir d'un niveau de référence de 0 volt. Ce niveau de référence est appelé terre de signalisation. Il est fondamental pour les équipements de transmission et de réception de données d'avoir le même point de référence de 0 volt. Si tel est le cas, ils sont mis à la terre de façon correcte.

Pour qu'un LAN fonctionne correctement, les équipements qui reçoivent des données doivent être capables d'interpréter précisément les 1 et les 0 transmis sous la forme de niveaux de tension. Les technologies Ethernet actuelles permettent d'atteindre des débits de plusieurs milliards de bits par seconde et chaque bit, d'une durée très réduite, doit être reconnu. Il est impossible d'amplifier la tension au niveau du récepteur, pas plus qu'il n'est possible d'étendre la durée d'un bit de façon à reconnaître les données. Cela signifie qu'un maximum de puissance du signal initial doit être conservé tout au long du trajet du signal via le câble et les connecteurs. En prévision de protocoles Ethernet plus rapides, les nouvelles installations doivent être équipées des meilleurs câbles, connecteurs et équipements d'interconnexion tels que les blocs de raccordement et les panneaux de brassage.

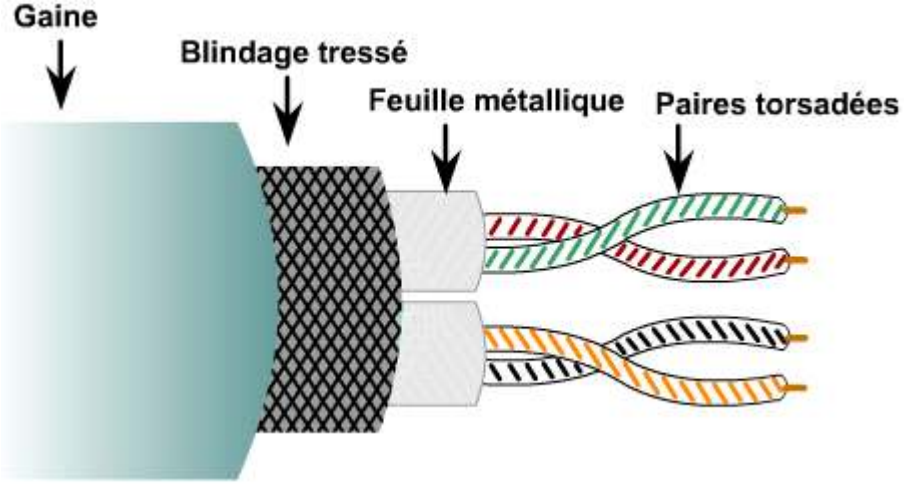
Les deux principaux types de câbles en cuivre sont les câbles blindés et les câbles non blindés. Dans les câbles blindés, le blindage protège les signaux de données des sources de bruit externes et des bruits générés par des signaux électriques à l'intérieur du câble.

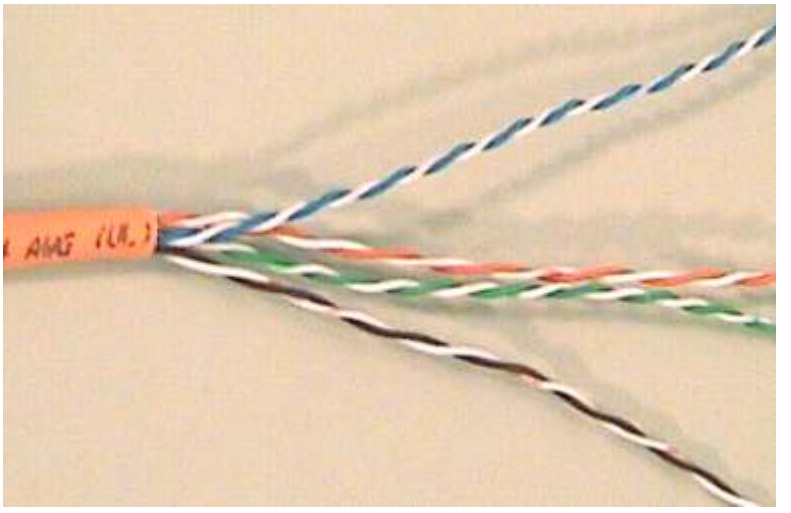
Le câble coaxial est un exemple de câble blindé. 1


Gaine extérieure
Blindage en cuivre tressé
Conducteur en cuivre
Isolant en plastique
Connecteur BNC
• Vitesse et débit : 10 à 100 Mbits/s
• Coût : Peu coûteux
• Taille du connecteur et du média : Moyenne
• Longueur de câble maximale : 500 m (moyen)

Il se compose d'un conducteur en cuivre monobrin entouré d'un matériau isolant et d'un blindage conducteur tressé. Dans les LAN, le blindage tressé est mis à la terre afin de protéger le conducteur interne du bruit électrique extérieur. Le blindage permet également de confiner le signal émis à l'intérieur du câble afin de réduire toute perte de signal. Les câbles coaxiaux sont ainsi moins bruyants que d'autres types de câbles en cuivre, mais ils sont également plus chers. En outre, ils sont plus difficiles à installer car ils prennent de la place, et il faut mettre le blindage à la terre.

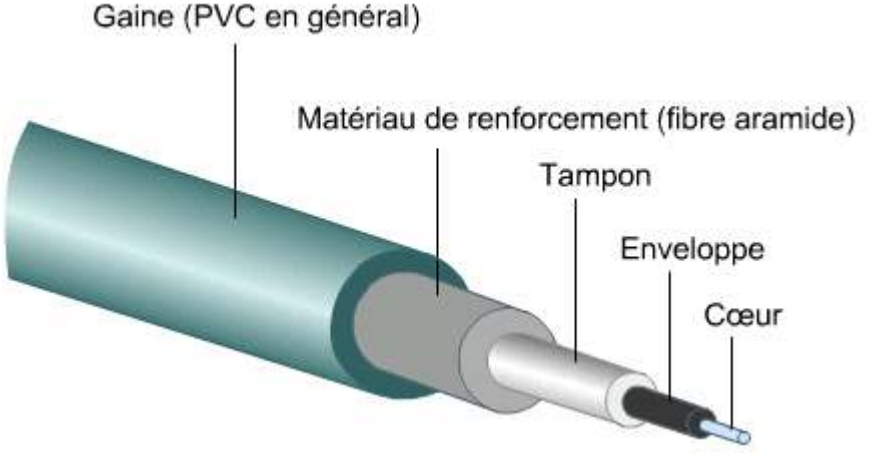
Il existe deux types de câbles à paires torsadées: les câbles à paires torsadées blindées (STP) et les câbles à paires torsadées non blindées (UTP). [2] [3]





Les câbles STP comprennent un blindage conducteur externe mis à la terre afin d'isoler les signaux du bruit électrique extérieur. Ils sont également composés de feuilles métalliques internes protégeant chaque paire du bruit généré par les autres paires. Les câbles STP sont parfois appelés à tort câbles ScTP (*screened twisted pair*). Les câbles ScTP sont en général des câbles à paires torsadées de catégorie 5 ou 5e, tandis que les câbles STP constituent un type de câble propre à IBM et ne contiennent que deux paires de conducteurs. Les câbles ScTP sont plus onéreux, plus difficiles à installer et d'usage moins fréquent que les câbles UTP. Ces derniers ne comportent pas de blindage et sont plus sensibles au bruit extérieur. Ce sont néanmoins les câbles les plus utilisés car ils sont moins onéreux et plus faciles à installer.

Dans un câble à fibre optique, l'intensité de la lumière augmente ou décroît afin de représenter les 1 et les 0 dans les transmissions de données. 4



Sur une même distance, la puissance d'un signal lumineux ne diminue pas autant que celle d'un signal électrique. Le bruit électrique n'affecte pas les signaux optiques. De plus, il n'est pas nécessaire de mettre la fibre optique à la terre, sauf si la gaine contient une substance métallique ou un élément de puissance métallique. Les câbles à fibre optique sont donc souvent utilisés pour relier des bâtiments entre eux ou les étages d'un même bâtiment. Les coûts de la fibre optique diminuant et sa vitesse de transmission augmentant, elle devrait devenir un média plus couramment utilisé pour les LAN.

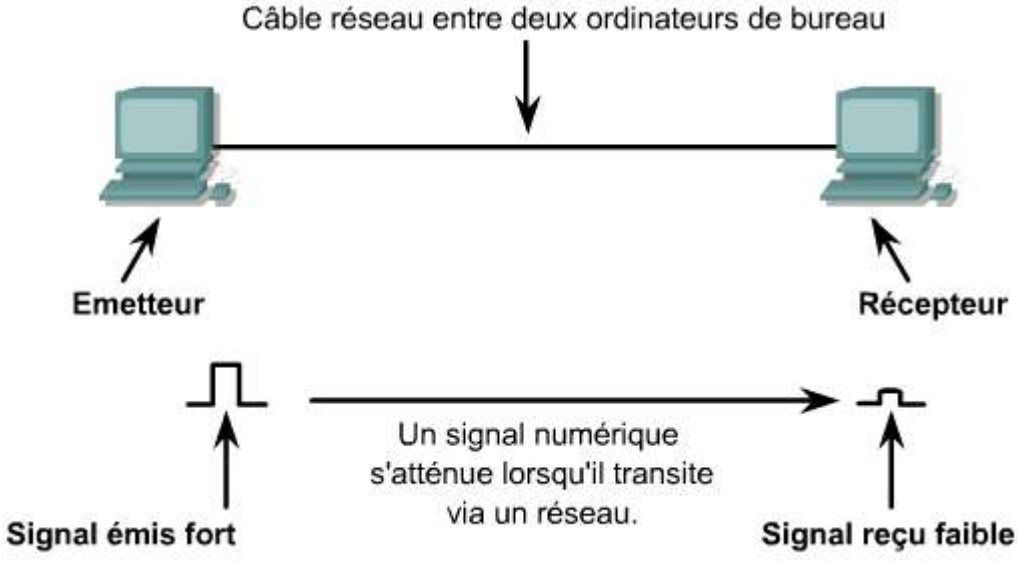
La page suivante explique le concept de l'affaiblissement d'insertion.

4.2 Signaux et bruits

4.2.2 Atténuation et affaiblissement d'insertion sur un média en cuivre

Cette page traite de l'affaiblissement d'insertion dû à une atténuation du signal et à des discontinuités d'impédance.

L'atténuation est la baisse d'amplitude du signal le long d'une liaison. Des câbles longs et des fréquences de signaux élevées contribuent à augmenter l'atténuation. C'est pourquoi l'atténuation se mesure à l'aide d'un testeur de câble réglé sur les fréquences les plus élevées que les câbles peuvent supporter. L'atténuation est exprimée en décibels (dB) par des nombres négatifs. Plus la valeur négative en décibels est petite, plus la performance de la liaison est bonne.



Plusieurs facteurs provoquent l'atténuation. La résistance du câble en cuivre convertit une partie de l'énergie électrique du signal en chaleur. De plus, l'énergie du signal se perd dans l'isolation du câble ainsi que dans l'impédance provoquée par des connecteurs défectueux.

L'impédance est la résistance opposée par le câble au courant alternatif (AC). Elle se mesure en ohms. L'impédance normale d'un câble de catégorie 5 est de 100 ohms. Si un connecteur n'est pas correctement installé sur un câble de catégorie 5, alors la valeur de son impédance sera différente de celle du câble. Cela est appelé discontinuité d'impédance ou défaut d'adaptation de l'impédance.

Les discontinuités d'impédance provoquent une atténuation car une partie du signal transmis est réfléchie, à la manière d'un écho, et n'atteint pas le récepteur. Cet effet se trouve accentué si de multiples discontinuités entraînent la réflexion de portions de signal supplémentaires vers l'émetteur. Lorsque le signal réfléchi rencontre la première discontinuité, une partie de ce signal repart vers son point de départ, ce qui crée un effet d'échos multiples. Les échos frappent donc le récepteur à différents intervalles de temps, ce qui lui complique la tâche pour détecter les valeurs des données. Ce phénomène est appelé « gigue » et provoque des erreurs dans les données.

La combinaison des effets de l'atténuation du signal et des discontinuités d'impédance sur une liaison de communication est appelée affaiblissement d'insertion. Le fonctionnement correct d'un réseau dépend d'une impédance caractéristique constante dans tous les câbles et les connecteurs, et de l'absence de discontinuités d'impédance à travers tout le système de câblage.

La page suivante traite des sources de bruit sur les câbles en cuivre.

4.2 Signaux et bruits

4.2.3 Sources de bruit sur les médias en cuivre

Cette page traite des sources de bruit sur les câbles en cuivre.

Le bruit est toute énergie électrique dans un câble de transmission qui rend difficile, pour le récepteur, l'interprétation des données venant de l'émetteur. La certification TIA/EIA-568-B exige désormais que les câbles soient testés pour différents types de bruits.

La diaphonie est la transmission des signaux d'un fil à un autre fil proche. Lorsque les tensions d'un fil changent, de l'énergie électromagnétique est générée. Cette énergie rayonne à partir du fil, à l'image d'un signal radio se propageant à partir d'un émetteur. Les fils adjacents dans le câble jouent le rôle d'antennes et reçoivent cette énergie, qui interfère avec leurs données. La diaphonie peut également être provoquée par des signaux provenant de câbles proches. Lorsque la diaphonie est provoquée par un signal émis par un autre câble, elle est appelée paradiaphonie étrangère. La diaphonie est plus néfaste sur des fréquences de transmission élevées.

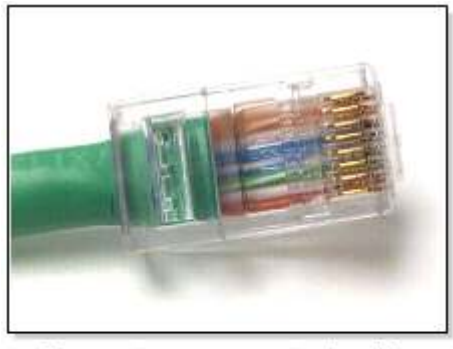
Les appareils de test des câbles mesurent la diaphonie en appliquant un signal test à l'une des paires. Le testeur de câble mesure ensuite l'amplitude des signaux de la diaphonie indésirable sur les autres paires de fils du câble.

Les câbles à paires torsadées sont conçus pour tirer parti des effets de la diaphonie afin de réduire au maximum le bruit. Dans les câbles à paires torsadées, une paire de fils est utilisée pour transmettre un seul signal. La paire de fils est torsadée pour que chaque fil subisse la même diaphonie. Puisqu'un signal de bruit apparaît sur l'un et l'autre fil de façon identique, ce bruit peut aisément être détecté et filtré au niveau du récepteur.

Les paires torsadées d'un câble sont également plus résistantes à la diaphonie ou aux signaux parasites provenant des paires adjacentes. Les câbles UTP des catégories supérieures sont dotés de paires aux torsades plus nombreuses afin de réduire la diaphonie pour les fréquences de transmission élevées. Lorsque les connecteurs sont raccordés aux extrémités de câbles UTP, les paires de fils doivent être détorsadées le moins possible afin d'assurer des communications fiables sur le LAN. 1



Connecteur incorrect : les fils sont détorsadés sur une trop grande longueur.



Connecteur correct : les fils sont détorsadés sur la longueur strictement nécessaire au raccordement du connecteur.

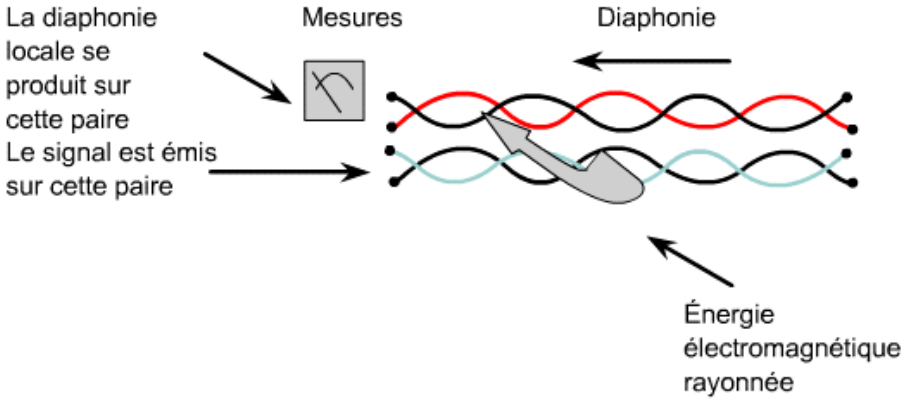
La page suivante présente les trois types de diaphonies.

4.2 Signaux et bruits
4.2.4 Types de diaphonies

Cette page définit les trois types de diaphonies.

- Diaphonie locale (NEXT)
- Diaphonie distante (FEXT)
- Diaphonie locale totale (PSNEXT)

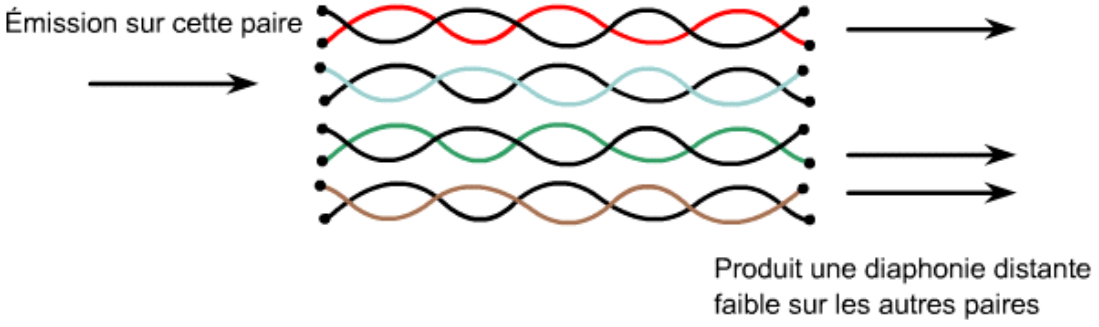
La diaphonie locale (NEXT) est calculée selon le rapport d'amplitude entre le signal test et le signal de diaphonie mesurés à la même extrémité de la liaison. [1] Cette différence est exprimée par une valeur négative en décibels (dB). Des valeurs négatives faibles indiquent une plus grande présence de bruit, tout comme des températures négatives faibles indiquent plus de chaleur. En règle générale, les testeurs de câbles n'affichent pas le signe moins indiquant une valeur de diaphonie locale négative. Une valeur de diaphonie locale affichée de 30 dB (qui signifie en fait –30 dB) indique un bruit de diaphonie locale moindre et un signal plus net qu'une valeur affichée de 10 dB.


La diaphonie locale se produit sur cette paire
Le signal est émis sur cette paire
Mesures
Diaphonie
Énergie électromagnétique rayonnée

La diaphonie locale doit être mesurée entre chaque paire et chacune des autres paires dans une liaison UTP, ainsi qu'à chacune de ses extrémités. Afin de réduire la durée des tests, certains appareils de test des câbles permettent à l'utilisateur de tester la performance de la diaphonie locale d'une liaison en utilisant des intervalles de fréquences plus grands que ceux spécifiés par la norme TIA/EIA. Néanmoins, les mesures obtenues se sont pas nécessairement conformes aux normes TIA/IEA-568-B et peuvent ne pas permettre de détecter toutes les défaillances d'une liaison. Afin de vérifier que la performance de la liaison est correcte, la diaphonie locale doit être mesurée à chaque extrémité de la liaison à l'aide d'un appareil de test de qualité. Il s'agit d'une condition nécessaire pour une conformité totale avec les normes pour câbles à haut débit.

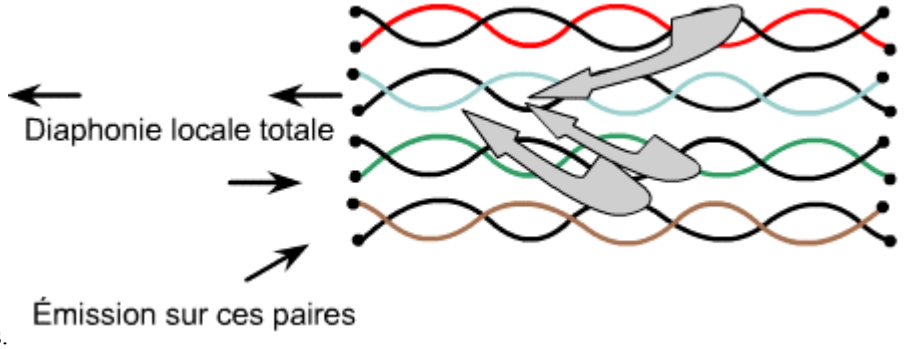
En raison de l'atténuation, une diaphonie intervenant à un point éloigné de l'émetteur crée moins de bruit sur un câble qu'une diaphonie locale. C'est une diaphonie distante, ou FEXT. [2] Le bruit occasionné par une diaphonie distante (FEXT) retourne lui aussi vers la source mais est atténué. Par conséquent, la diaphonie

distante n'est pas aussi problématique que la diaphonie locale.



La diaphonie locale totale (PSNEXT) mesure l'effet cumulé d'une diaphonie locale provenant de toutes les paires d'un câble. [3] Pour chaque paire, la diaphonie locale totale se calcule selon les effets de diaphonie locale des trois autres paires. L'effet combiné de la diaphonie provenant de sources de transmission simultanées multiples peut être très nuisible pour le signal. La certification TIA/EIA-568-B exige désormais ce test de diaphonie locale totale.

Certains standards Ethernet comme 10BaseT et 100BaseTX reçoivent des données à partir d'une seule paire de fils par direction. Cependant, pour des technologies plus récentes telles que 1000BaseT, qui reçoivent des données simultanément à partir de paires multiples dans la même direction, les tests de diaphonie totale sont très importants.



La page suivante traite des normes de test des câbles.

4.2 Signaux et bruits

4.2.5 Normes de test des câbles

Cette page présente la norme TIA/EIA-568-B. Cette norme préconise dix tests à faire passer à un câble de cuivre s'il doit être utilisé sur des LAN Ethernet modernes à haut débit.

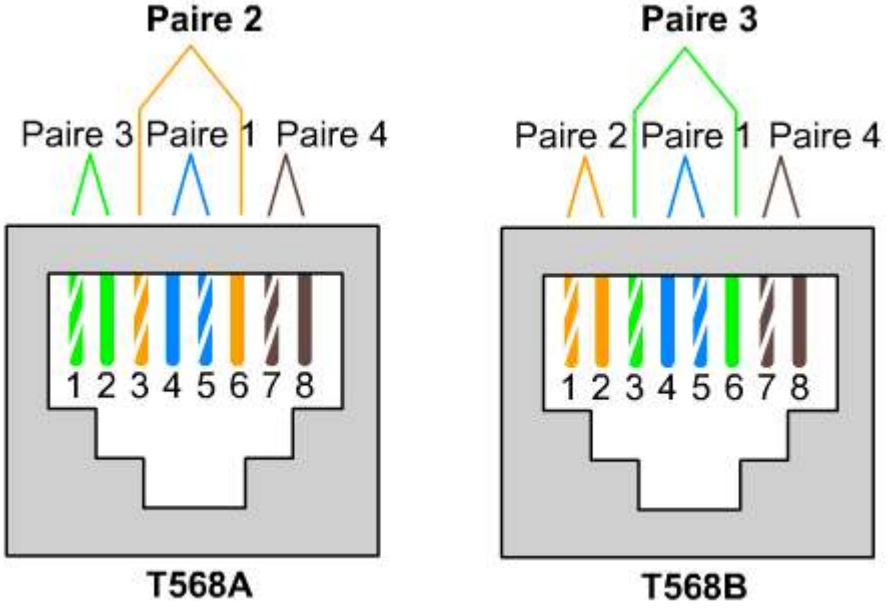
Toutes les liaisons par câble doivent être testées avec le débit maximum qui peut être appliqué à la catégorie de câble à installer.

Les dix paramètres de test fondamentaux à vérifier pour qu'une liaison par câble soit conforme aux normes TIA/EIA sont les suivants:

- le schéma de câblage,
- l'affaiblissement d'insertion,
- la diaphonie locale (NEXT),
- la diaphonie locale totale (PSNEXT),

- la diaphonie distante de niveau égal (ELFEXT),
- la diaphonie distante totale de niveau égal (PSELFEXT),
- la perte de retour,
- le délai de propagation,
- la longueur de câble,
- la distorsion du délai.

La norme Ethernet stipule que chaque broche d'un connecteur RJ-45 a une finalité particulière. 1



Une carte réseau transmet des signaux sur les broches 1 et 2, puis reçoit d'autres signaux sur les broches 3 et 6. Les fils d'un câble UTP doivent être connectés aux broches correspondantes à chaque extrémité d'un câble. 2

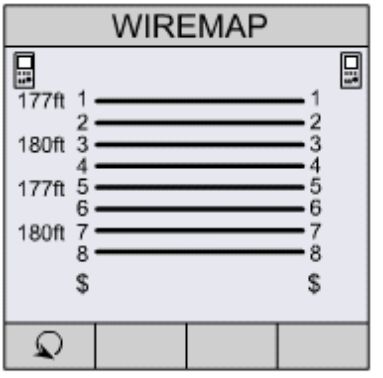
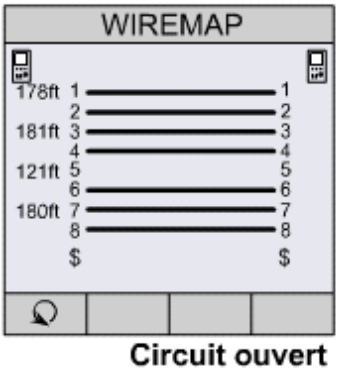
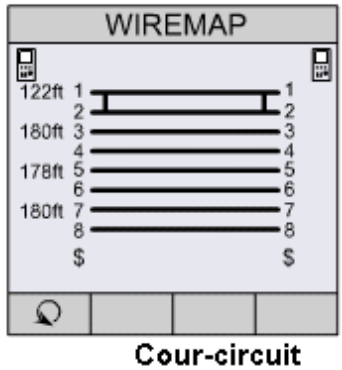


Schéma de câblage correct



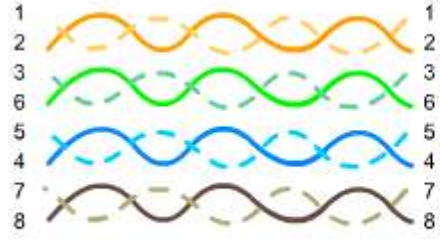
Circuit ouvert



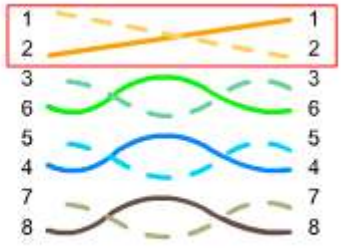
Cour-circuit

Le test de schéma de câblage garantit qu'il n'y a aucun circuit ouvert ou court-circuit sur le câble. Un circuit est ouvert lorsque le fil n'est pas correctement raccordé au connecteur. Un court-circuit se produit lorsque deux fils sont connectés entre eux.

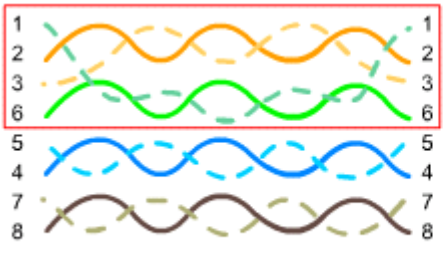
Le test de schéma de câblage permet également de vérifier que les huit fils sont raccordés aux broches correspondantes, et ce, aux deux extrémités du câble. Il existe différentes erreurs de câblage que le test de schéma de câblage est capable de détecter. 3



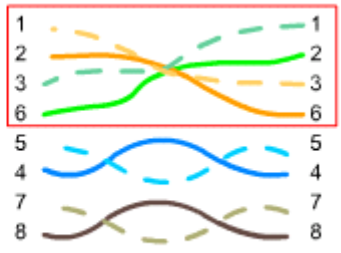
Câblage T568B correct



Erreur de paires inversées



Erreur de paires séparées



Erreur de paires croisées

Les erreurs de paires inversées se produisent lorsqu'une paire est correctement installée sur l'un des connecteurs mais inversée sur l'autre. Par exemple, si le fil blanc et orange est raccordé à la broche 1, et le fil orange à la broche 2 à l'une des extrémités du câble, mais que le raccordement est inversé à l'autre extrémité, il s'agit d'une erreur de paires inversées. Cet exemple est illustré par la figure.

Il s'agit d'une erreur de paires séparées lorsque l'un des fils d'une paire est commuté avec un fil d'une autre paire aux deux extrémités du câble. Observez attentivement les numéros des broches sur la figure afin de détecter l'erreur de câblage. Une paire séparée crée deux paires émettrices ou réceptrices, chacune possédant deux fils qui ne sont pas torsadés ensemble. Cette erreur gêne le processus d'annulation et rend le câble plus sensible à la diaphonie et aux interférences. Comparez cette erreur avec l'erreur des paires inversées, où la même paire de broches est utilisée à chaque extrémité.

D'autres paramètres de tests sont décrits à la page suivante.

4.2 Signaux et bruits

4.2.6 Autres paramètres de tests

Cette page présente les tests des câbles pour la diaphonie et l'atténuation. 1

- La diaphonie se mesure par quatre tests différents.
- Un testeur de câble mesure la diaphonie locale en appliquant un signal test à une paire
- Le test de diaphonie distante de niveau égal (ELFEXT) mesure la diaphonie distante (FEXT)
- La diaphonie distante totale de niveau égal (PSELFEXT) est l'effet combiné de la diaphonie distante de niveau égal de toutes les paires de fils

La combinaison des effets de l'atténuation du signal et des discontinuités d'impédance sur une liaison de communication est appelée affaiblissement d'insertion. L'affaiblissement d'insertion est mesuré en décibels à l'extrémité éloignée du câble. Les normes TIA/EIA stipulent qu'il faut effectuer un test d'affaiblissement d'insertion sur un câble et ses connecteurs avant d'utiliser le câble en tant que liaison dans un LAN.

La diaphonie se mesure par quatre tests différents. Un testeur de câble mesure la diaphonie locale en appliquant un signal test à l'une des paires du câble et en mesurant l'amplitude du signal de diaphonie reçu par les autres paires du câble. La valeur de la diaphonie locale, exprimée en décibels, est calculée selon la différence d'amplitude entre le signal test et le signal de diaphonie mesurés à la même extrémité de la liaison. Rappelez-vous que le nombre de décibels indiqués par le testeur est un nombre négatif et que par conséquent, plus il est élevé, plus la diaphonie de la paire de fils est faible. Comme indiqué précédemment, le test de diaphonie locale totale se calcule en se basant sur les effets combinés de la diaphonie locale.

Le test de diaphonie distante de niveau égal (ELFEXT) mesure la diaphonie distante (FEXT). La diaphonie distante de niveau égal de paire à paire est exprimée en décibels. Elle représente la différence entre la diaphonie distante et l'affaiblissement d'insertion de la paire dont le signal est perturbé par la diaphonie distante. La diaphonie distante de niveau égal est une mesure importante sur les réseaux Ethernet utilisant les technologies 1000BaseT. La diaphonie distante totale de niveau égal (PSELFEXT) est l'effet combiné de la diaphonie distante de niveau égal de toutes les paires de fils.

La perte de retour, exprimée en décibels, mesure les réflexions dues aux discontinuités d'impédance à n'importe quel point de la liaison. Souvenez-vous que la conséquence principale d'une perte de retour n'est pas la perte de puissance du signal. Le problème central réside dans le fait que les échos provoqués par les

réflexions dues aux discontinuités d'impédance frappent le récepteur à différents intervalles et entraînent une gigue du signal.

La page suivante aborde le concept du délai de propagation.

4.2 Signaux et bruits

4.2.7 Paramètres basés sur le temps

Cette page porte sur le délai de propagation et explique comment le mesurer.

Le délai de propagation est une mesure simple du temps que met un signal à transiter le long d'un câble en cours de test. Dans une paire de fils, ce délai dépend de la longueur des fils, de leurs propriétés électriques et du nombre de torsades par mètre de câble. Les délais de propagation s'expriment en centièmes de nanosecondes. Une nanoseconde représente un milliardième de seconde, soit 0,000000001 seconde. La norme TIA/EIA-568-B impose une limite pour les délais de propagation selon les différentes catégories de câbles UTP.

C'est à partir des mesures de délai de propagation qu'est calculée la longueur des câbles. La norme TIA/EIA-568-B.1 stipule que la longueur physique d'une liaison doit être calculée sur la paire dont le délai électrique est le plus court. Les testeurs mesurent la longueur d'un fil selon le délai électrique établi par un test de réflectométrie (TDR), et non pas selon la longueur physique de la gaine du câble. Les paires à l'intérieur des câbles étant torsadées, les signaux se propagent en réalité sur une distance supérieure à celle physiquement parcourue par le câble. Lorsqu'un testeur de câble effectue une mesure de réflectométrie, il envoie un signal sous forme d'impulsion dans une paire de fils et calcule le temps de retour de l'impulsion sur cette même paire.

Le test de réflectométrie n'est pas seulement utilisé pour déterminer la longueur d'un câble mais aussi pour évaluer la distance qui sépare un point d'une défaillance (par exemple, un court-circuit, un circuit ouvert, etc.). Lorsque l'impulsion rencontre un court-circuit, un circuit ouvert ou une mauvaise connexion, tout ou partie de l'énergie de l'impulsion est réfléchie vers le testeur. Cela permet de calculer la distance approximative à parcourir pour atteindre la défaillance. Cette distance sert à localiser un point de connexion défaillant sur le parcours du câble, une prise murale par exemple.

Les délais de propagation des différentes paires dans un câble unique peuvent varier quelque peu en fonction des différences dans le nombre de torsades et dans les propriétés électriques de chaque paire. La différence de délai entre les paires est appelée distorsion de délai. La distorsion de délai est un paramètre fondamental pour des réseaux à haut débit, comme Ethernet 1000BaseT, où les données sont transmises simultanément par des paires multiples. Si la distorsion de délai entre les paires est trop grande, les bits n'arrivent pas en même temps et les données ne peuvent pas être correctement reconstituées. Même si une liaison câblée n'est pas destinée à ce type de transmission de données, le test du délai de distorsion doit faire en sorte que la liaison puisse supporter des mises à jour à venir pour un réseau à haut débit.

Toutes les liaisons par câble d'un LAN doivent passer tous les tests mentionnés plus haut (spécifiés dans la norme TIA/EIA-568-B) afin d'être considérées comme conformes aux normes. Un testeur de certification doit être utilisé afin d'assurer que la liaison a bien été soumise à tous les tests et est conforme à la norme. Ces tests garantissent le fonctionnement de la liaison à des débits et des fréquences élevés. Les tests de câbles doivent être effectués lors de l'installation du câble, puis régulièrement, afin de garantir que le câblage du LAN est conforme aux normes de l'industrie. Les appareils de test des câbles doivent être de haute qualité et être utilisés correctement afin de garantir la précision des tests. Les résultats des tests doivent également être soigneusement

notés.

- Le délai de propagation est une mesure simple du temps que met un signal à transiter le long d'un câble en cours de test.
- Les délais de propagation s'expriment en centièmes de nanosecondes.
- La norme TIA/EIA-568-B impose une limite pour les délais de propagation selon les différentes catégories de câbles UTP.
- La différence de délai entre les paires est appelée distorsion de délai.

La page suivante décrit la procédure de test des médias optiques.

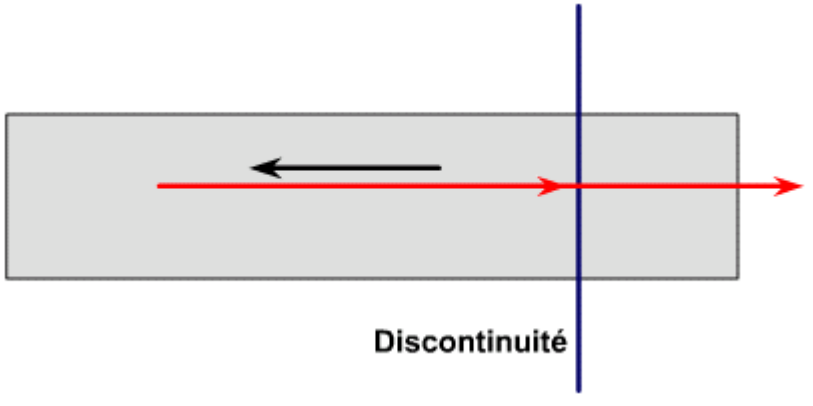
4.2 Signaux et bruits

4.2.8 Test des médias à fibre optique

Cette page décrit la procédure de test des médias à fibre optique.

Une liaison à fibre optique est constituée de deux fibres de verre séparées acheminant les données indépendamment l'une de l'autre. L'une des deux fibres transporte les signaux émis dans une direction, tandis que la seconde les transporte dans la direction opposée. Chaque fibre de verre est entourée d'une gaine à travers laquelle la lumière ne peut pas passer. Il n'existe donc pas de problèmes de diaphonie pour des câbles à fibre optique. Les interférences électromagnétiques ou le bruit à l'extérieur n'ont pas d'impact sur le câblage optique. Néanmoins, les liaisons à fibre optique sont sensibles à l'atténuation, mais dans une moindre mesure que les câbles en cuivre.

Les liaisons en fibre optique sont sujettes à l'équivalent optique des discontinuités d'impédance observées sur les câbles à paires torsadées non blindées. [1]



Lorsque la lumière rencontre une discontinuité optique, une partie du signal lumineux est réfléchie dans la direction opposée et seule une fraction du signal lumineux initial continue à parcourir la fibre jusqu'au récepteur. Cela débouche sur une réduction de la quantité d'énergie lumineuse parvenant au récepteur et sur des difficultés de reconnaissance du signal. Tout comme pour les câbles UTP, des connecteurs mal installés sont la principale cause d'une réflexion de la lumière et d'une perte de puissance du signal dans la fibre optique.

Le bruit ne posant pas de problèmes lors d'une transmission par fibre optique, la préoccupation principale pour une liaison optique est la puissance du signal lumineux parvenant au récepteur. L'atténuation affaiblissant le signal lumineux au niveau du récepteur, des erreurs de données peuvent survenir. Tester un câble à fibre optique implique tout d'abord d'acheminer de la lumière le long du câble et de s'assurer qu'une quantité de lumière suffisante parvient jusqu'au récepteur.

Sur une liaison à fibre optique, il faut calculer la quantité de perte de puissance d'un signal acceptable, sans descendre au-dessous du minimum requis par le récepteur. C'est ce que l'on appelle le budget d'une liaison à fibre optique. Un appareil pour tester les fibres optiques, connu sous le nom de source de lumière et mesureur de puissance, vérifie si le budget optique d'une liaison est dépassé. 2



Si le résultat du test est négatif, un autre appareil de test des câbles peut être utilisé pour localiser les discontinuités optiques sur le parcours du câble. Un réflectomètre optique (OTDR) permet de localiser ces discontinuités. En général, le problème est dû à un ou plusieurs connecteurs mal raccordés. Le réflectomètre optique localise les connexions défaillantes à remplacer. Lorsque les défaillances sont réparées, le câble doit être soumis à un nouveau test.

Les normes de test sont mises à jour régulièrement. La page suivante contient des informations sur une nouvelle norme.

4.2 Signaux et bruits

4.2.9 Nouvelle norme

Cette page introduit les nouvelles normes de test pour les câbles de catégorie 6.

Le supplément pour les câbles de catégorie 6 a été ajouté à la norme TIA-568 le 20 juin 2002. L'intitulé officiel de la norme est le suivant : ANSI/TIA/EIA-568-B.2-1. Celle-ci indique l'ensemble des paramètres de performance de base qui doivent être testés pour un câblage Ethernet, ainsi que les résultats qui doivent être obtenus pour être en conformité avec la norme. Les câbles certifiés de catégorie 6 doivent passer les dix tests avec succès.

Bien que les tests de la catégorie 6 soient pour l'essentiel les mêmes que ceux de la catégorie 5, les câbles de catégorie 6 doivent obtenir des résultats supérieurs afin d'obtenir la certification. Les câbles de catégorie 6 doivent pouvoir supporter des fréquences allant jusqu'à 250 MHz et leurs niveaux de diaphonie et de perte de retour doivent être plus faibles.



Un testeur de câble de qualité similaire au Fluke DSP-4000 ou au Fluke OMNIScanner2 peut effectuer toutes les mesures requises pour la certification des câbles des catégories 5, 5e et 6 sur des liaisons permanentes ou des liaisons de canal. La figure 1

montre un analyseur de câble Fluke DSP-4100 avec un adaptateur canal/trafic DSP-LIA013 pour la catégorie 5e.

Les activités de TP portent sur l'utilisation d'un testeur de câble.

Cette leçon est terminée. La page suivante récapitule les principaux points évoqués au cours de ce module.



Activité de TP

Exercice: Testeur de câble Fluke 620 – Schéma de câblage

Au cours de ce TP, vous allez apprendre à utiliser la fonction de mappage des fils du câblomètre LAN Fluke 620 (ou d'un appareil équivalent).



Activité de TP

Exercice: Testeur de câble Fluke 620 – Erreurs de câblage

Au cours de ce TP, vous allez apprendre les fonctions de réussite/d'échec aux tests du câblomètre LAN Fluke 620 (ou d'un appareil équivalent).



Activité de TP

Exercice: Testeur de câble Fluke 620 – Longueur

Au cours de ce TP, vous allez apprendre à utiliser la fonction de mesure de longueur de câble du câblomètre LAN Fluke 620 (ou d'un appareil équivalent).



Activité de TP

Exercice: LinkRunner Fluke – Tests sur réseau LAN

Au cours de ce TP, vous allez vous familiariser avec les fonctionnalités du LinkRunner Fluke et déterminer si un branchement est actif.



Activité de TP

Exercice: LinkRunner Fluke – Tests des câbles et de la carte réseau

Au cours de ce TP, vous allez vous familiariser avec les fonctionnalités du LinkRunner Fluke et vérifier la longueur du câble ainsi que son intégrité.

Résumé

Cette page récapitule les thèmes abordés tout au long du module.

Des données symbolisant des caractères, des mots, des images, des vidéos ou de la musique peuvent être représentées de manière électrique par des variations de tension dans des câbles ou autres équipements électroniques. Les données que ces variations de tension représentent peuvent être converties en ondes lumineuses ou radioélectriques, puis à nouveau en variations de tension. Les ondes sont de l'énergie qui circule d'un endroit à l'autre et sont provoquées par des perturbations. Elles ont toutes des propriétés communes telles que l'amplitude, la période et la fréquence. Les ondes sinusoïdales sont des fonctions périodiques, variant continuellement en fonction du temps. Les signaux analogiques sont semblables à des ondes sinusoïdales. Les ondes carrées sont des fonctions périodiques dont les valeurs restent constantes durant un certain temps avant de changer brusquement. Les signaux numériques sont semblables à des ondes carrées.

Les exposants sont utilisés pour représenter des nombres très grands ou très petits. Un nombre élevé à une puissance positive est égal à ce nombre multiplié par lui-même autant de fois que l'indique l'exposant. Par

exemple, 10^3 = 10x10x10 = 1000. Les logarithmes fonctionnent de la même manière que les exposants. Le logarithme de base 10 d'un nombre est égal à la puissance à laquelle il faut élever 10 pour obtenir le nombre. Par exemple, log10 1000 = 3 car 10^3 = 1000.

Les décibels permettent de mesurer le gain ou la perte de puissance d'un signal. Les valeurs négatives représentent des pertes, et les valeurs positives, des gains. L'analyse du temps et de la fréquence peut être utilisée pour tracer la courbe de la tension ou de la puissance d'un signal.

Des signaux parasites dans un système de communication sont appelés bruit. Le bruit provient d'autres câbles, d'interférences radioélectriques (RFI) et d'interférences électromagnétiques (EMI). Le bruit peut affecter toutes les fréquences de signaux ou une partie d'entre elles.

La bande passante analogique est la plage de fréquences de certaines transmissions analogiques (télévision, radio FM, etc.). Elle mesure la quantité de données pouvant circuler d'un endroit à un autre pendant une période donnée. Elle s'exprime en plusieurs multiples de bits par seconde.

Dans les câbles en cuivre, les signaux de données correspondent à des niveaux de tension représentés de façon binaire par des 1 et des 0. Afin que le LAN fonctionne normalement, l'équipement de réception doit être en mesure d'interpréter précisément le signal en bits. Un câblage correctement installé et conforme aux normes augmente la fiabilité et les performances du LAN.

La dégradation d'un signal est due à des facteurs tels que l'atténuation, le défaut d'adaptation de l'impédance, le bruit, ainsi que plusieurs types de diaphonies. L'atténuation est la baisse d'amplitude du signal le long d'une liaison. L'impédance est la mesure d'une résistance à un signal électrique. Les câbles et leurs connecteurs doivent avoir des valeurs d'impédance similaires pour que le signal de données ne soit pas partiellement réfléchi par le connecteur. Ce phénomène est appelé défaut d'adaptation de l'impédance ou discontinuité d'impédance. Le bruit est toute énergie électrique dans un câble de transmission qui rend difficile, pour le récepteur, l'interprétation des données venant de l'émetteur. La diaphonie est la transmission des signaux d'un fil à un autre fil proche. Il existe trois types de diaphonies : La diaphonie locale (NEXT), la diaphonie distante (FEXT) et la diaphonie locale totale (PSNEXT).

Les câbles STP et UTP sont conçus pour tirer parti des effets de la diaphonie afin de réduire au maximum le bruit. En outre, les câbles STP sont composés d'une gaine conductrice externe et de feuilles métalliques internes les rendant moins sensibles au bruit. Ces câbles ne comportent pas de blindage et sont plus sensibles au bruit extérieur. Ce sont néanmoins les câbles les plus utilisés car ils sont moins onéreux et plus faciles à installer.

Les câbles à fibre optique sont utilisés pour transmettre des signaux de données en augmentant ou en diminuant l'intensité de la lumière afin de représenter les 1 et les 0 dans les transmissions. Sur une même distance, la puissance d'un signal lumineux ne diminue pas de la même façon que celle d'un signal électrique. Le bruit n'affecte pas les signaux optiques et il n'est pas nécessaire de mettre la fibre optique à la terre. Les câbles à fibre optique sont donc souvent utilisés pour relier des bâtiments entre eux ou les étages d'un même bâtiment.

La norme TIA/EIA-568-B préconise dix tests à faire passer à un câble de cuivre s'il doit être utilisé sur des LAN Ethernet modernes à haut débit. Les câbles à fibre optique doivent également être testés selon les normes applicables aux réseaux. Les câbles de catégorie 6 requièrent des normes de tests de fréquence plus sévères que les câbles de catégorie 5.

Résumé

- Les tests de câbles impliquent de connaître certains concepts électriques et mathématiques ainsi que des termes comme signal, onde, fréquence et bruit. Il est utile de comprendre ces notions lors d'une formation sur les réseaux, le câblage et les tests de câbles.
- L'atténuation (affaiblissement d'un signal) et le bruit (signal parasite) peuvent poser des problèmes sur les réseaux car les données reçues ne sont pas toujours reconnues. Il est important que le raccordement des connecteurs de câbles et l'installation des câbles soient correctement effectués.

5-Cablâge des réseaux lan et wan

Vue d'ensemble

Bien que chaque réseau LAN soit unique, tous les réseaux LAN possèdent des points communs en matière de conception. Par exemple, la plupart des réseaux LAN utilisent des normes et des composants identiques. Ce module traite de certains éléments des réseaux LAN Ethernet et présente les équipements LAN courants. Il existe plusieurs types de connexions WAN. Pouvant faire appel à des modes d'accès aussi divers que l'accès commuté ou à large bande, ces connexions diffèrent sur le plan de la bande passante, du coût et de l'équipement requis. Ce module présente les différents types de connexions WAN.

Ce module traite, par ailleurs, certains objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco • Sélection de services WAN répondant aux besoins des clients	• Mise en œuvre d'un LAN		

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception ou modification d'un LAN simple à l'aide de produits Cisco • Conception d'un interréseau simple à l'aide de produits Cisco	• Mise en œuvre d'un LAN		• Évaluation des caractéristiques des environnements LAN • Évaluation des principales caractéristiques des technologies HDLC, PPP, Frame Relay, DDR, et RNIS

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Description et installation du matériel et du logiciel requis pour pouvoir communiquer via un réseau • Établissement de communication entre un équipement terminal et l'IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système	• Description des topologies et des problèmes physiques liés au câblage des réseaux LAN les plus répandus • Identification des principales caractéristiques des technologies et des configurations WAN (Wide Area Networking) courantes, et différences par rapport aux technologies LAN les plus répandues • Description du matériel et du logiciel requis pour pouvoir communiquer via un réseau • Description des normes et des propriétés physiques, électriques et mécaniques liées aux médias optiques, sans fil et en cuivre utilisés dans les réseaux • Description du rôle d'un routeur dans un WAN

Au terme de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
5.1	Câblage des réseaux LAN
5.2	Câblage des réseaux WAN

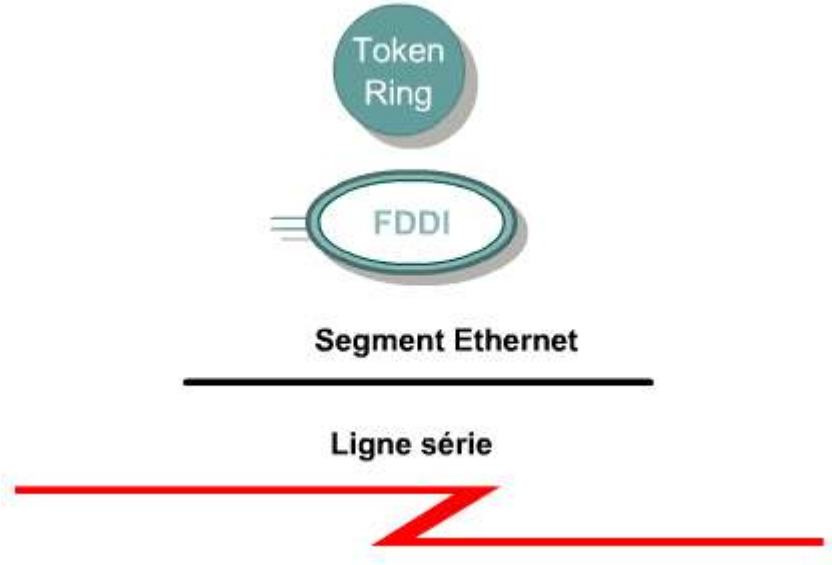
- Identifier les caractéristiques des réseaux Ethernet
- Identifier les câbles droits, croisés et à paires inversées
- Décrire la fonction, les avantages et les inconvénients des répéteurs, des concentrateurs, des ponts, des commutateurs et des composants réseau sans fil
- Décrire la fonction des réseaux d'égal à égal
- Décrire la fonction, les avantages et les inconvénients des réseaux client-serveur
- Décrire et identifier les différents types de connexions WAN (série, RNIS, DSL et modem câble)
- Identifier les ports série, les câbles et les connecteurs des routeurs
- Identifier et décrire l'emplacement de l'équipement utilisé dans les différentes configurations WAN

5.1 Câblage des réseaux LAN

5.1.1 Couche physique des réseaux LAN

Cette page présente la couche physique des réseaux LAN.

Différents symboles sont utilisés pour représenter les types de média. Le réseau Token Ring est représenté par un cercle. Le réseau FDDI est représenté par deux cercles concentriques et le réseau Ethernet symbolisé par une ligne droite. Les connexions série sont représentées par une ligne en forme d'éclair. 1



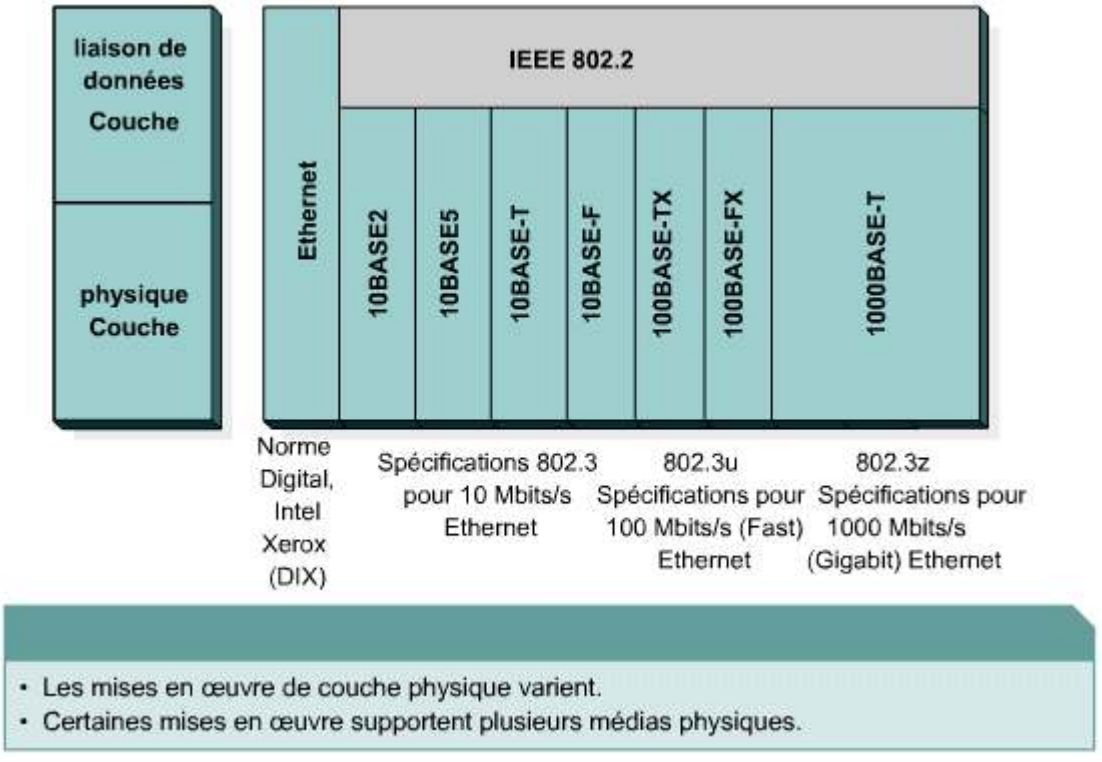
Vous pouvez faire appel à plusieurs types de média pour concevoir un réseau informatique. Un média permet d'acheminer un flux d'informations via un réseau LAN. Les LAN sans fil utilisent l'atmosphère ou l'espace comme média. Les autres médias réseau confinent les signaux réseau dans des fils, des câbles ou de la fibre

optique. Les médias réseau sont considérés comme des composants de la couche 1 (ou couche physique) des réseaux LAN.

Chaque type de média présente des avantages et des inconvénients, basés sur les facteurs suivants :

- La longueur de câble
- Le coût
- La facilité d'installation
- La sensibilité aux interférences

Le câble coaxial, la fibre optique et l'espace peuvent transporter les signaux réseau. Ce module est plus particulièrement consacré aux câbles UTP de catégorie 5, dont la famille de câbles de catégorie 5e. De nombreuses topologies prennent en charge les réseaux LAN, au même titre que d'autres médias physiques. La figure 2



montre un sous-ensemble des mises en œuvre de couche physique pouvant être déployées pour la prise en charge d'Ethernet.

La page suivante décrit la mise en œuvre d'Ethernet dans un environnement de type campus.

5.1 Câblage des réseaux LAN

5.1.2 Ethernet dans le campus

Cette page traite d'Ethernet.

Ethernet est la technologie LAN la plus répandue. Le groupe DIX (*Digital, Intel et Xerox*) a été le premier à la mettre en œuvre. DIX a créé et mis en œuvre la première spécification LAN Ethernet, qui a servi de base à l'élaboration de la norme 802.3 de l'IEEE (*Institute of Electrical and Electronics Engineers*) introduite en 1980. L'IEEE a étendu la norme 802.3 à trois nouveaux comités : 802.3u pour Fast Ethernet, 802.3z pour Gigabit Ethernet sur fibre optique et 802.3ab pour Gigabit Ethernet sur câble à paires torsadées non blindées.

Un réseau peut nécessiter une mise à niveau vers une topologie Ethernet plus rapide. La plupart des réseaux Ethernet prennent en charge des débits de 10 Mbits/s et 100 Mbits/s.

La nouvelle génération de produits multimédia, de traitement d'images et de bases de données peut facilement submerger un réseau assurant des débits Ethernet classiques de 10 et 100 Mbits/s. Les administrateurs réseau ont alors la possibilité de mettre en œuvre une interface Gigabit Ethernet du backbone à l'utilisateur final. 1

	Mise en œuvre Ethernet 10BaseT	Mise en œuvre Fast Ethernet	Mise en œuvre Gigabit Ethernet
Niveau utilisateur final (de l'équipement utilisateur final vers l'équipement	Permet une connectivité pour les applications de petite taille et de taille	Permet un accès à 100-Mbits/s au serveur pour les stations de travail hautes performances.	Généralement pas utilisé à ce niveau.
Niveau groupe de travail (de l'équipement groupe de travail au backbone)	Généralement pas utilisé à ce niveau.	Permet la connectivité entre l'utilisateur final et les groupes de travail. Permet la connectivité du groupe de travail au backbone. Permet la connectivité du bloc serveur à la couche backbone.	Permet une connectivité hautes performances au bloc serveur de l'entreprise.
Niveau backbone	Généralement pas utilisé à ce niveau.	Permet la connectivité du bloc serveur groupe de travail au backbone.	Permet une connectivité haut débit pour l'équipement du réseau et le backbone.

Les coûts d'installation des nouveaux câbles et adaptateurs peuvent toutefois constituer un frein.

Les technologies Ethernet peuvent être utilisées de différentes façons dans un réseau de type campus :

- La mise en place d'un débit Ethernet de 10 Mbits/s au niveau des utilisateurs permet d'obtenir des performances satisfaisantes. Les clients ou les serveurs qui ont besoin d'une bande passante plus importante peuvent utiliser un débit Ethernet de 100 Mbits/s.
- L'interface Fast Ethernet constitue la liaison entre les équipements utilisateur et réseau. Elle prend en charge la totalité du trafic généré sur chaque segment Ethernet.
- La technologie Fast Ethernet peut servir à relier des serveurs d'entreprise. Ainsi, elle optimise la performance client-serveur sur le réseau du campus tout en permettant d'éviter les goulots d'étranglement.
- Selon les moyens financiers mis en œuvre, il est possible de relier les équipements du backbone via une interface Fast Ethernet ou Gigabit Ethernet.

Les médias et les connecteurs à utiliser dans le cadre de la mise en œuvre d'Ethernet sont abordés dans la page suivante.

5.1 Câblage des réseaux LAN

5.1.3 Besoins en médias et connecteurs Ethernet

Cette page traite des points à prendre en compte pour la mise en œuvre d'Ethernet. Il s'agit notamment des besoins en médias et en connecteurs et du niveau de performance du réseau.

En matière de câbles et de connecteurs, les spécifications utilisées pour la prise en charge des implémentations Ethernet sont dérivées des normes EIA/TIA. Les catégories de câbles spécifiques d'Ethernet sont basées sur les normes de télécommunications relatives aux édifices commerciaux EIA/TIA-568 SP-2840.

La figure 1 compare les spécifications de câbles et de connecteurs relatives aux implémentations Ethernet classiques. Il est important de remarquer les médias pouvant être utilisés pour Ethernet 10 Mbits/s versus Ethernet 100 Mbits/s. Les réseaux comportant une combinaison de débits 10 Mbits/s et 100 Mbits/s doivent avoir recourt à la catégorie de câble UTP 5e ou supérieure afin de supporter Fast Ethernet.

La page suivante traite des différents types de connexion.

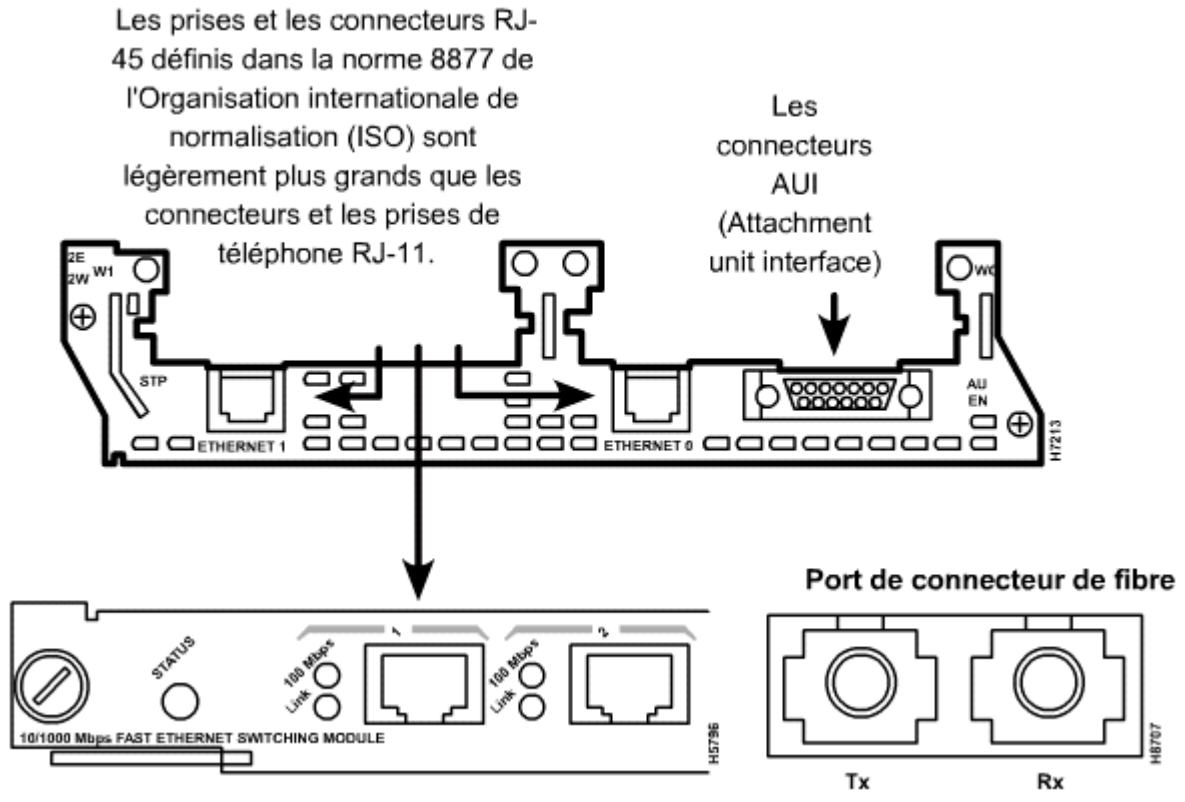
	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Médias	Câble coaxial de 50 ohms (Ethernet à câble fin)	Câble coaxial de 50 ohms (Ethernet épais)	Câble EIA/TIA Catégorie 3, 4, 5 UTP, deux paires	Câble EIA/TIA Catégorie 5 UTP, deux paires	Fibre multimode de 62,5/125
Longueur maximale du segment	185 m	500 m	100 m	100 m	400 m
Topologie	En bus	En bus	En étoile	En étoile	En étoile
Connecteur	BNC	AUI (Attachment Unit Interface)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur d'interface média duplex Connecteur ST ou SC

1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
STP	Câble EIA/TIA catégorie 5 UTP, quatre paires	Fibre multimode de 62,5/50 microns.	Fibre multimode de 62,5/50 microns ; fibre monomode de 9 microns.
25 m	100 m	275 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns	440 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns ; de 3 à 10 km pour la fibre monomode.
En étoile	En étoile	En étoile	En étoile
ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur SC	Connecteur SC

5.1 Câblage des réseaux LAN

5.1.4 Média de connexion

Cette page décrit les différents types de connexion possibles au niveau de la couche physique, précédemment illustrés par la figure 1



En termes de connecteur et de prise, le modèle RJ-45 est le plus répandu. Les connecteurs RJ-45 sont décrits plus en détail dans la section suivante.

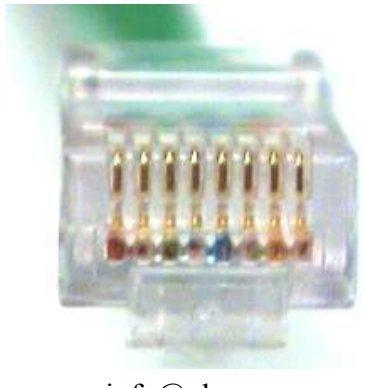
Le connecteur d'une carte réseau peut ne pas correspondre au média auquel il doit être relié. Comme le montre la figure 1, il peut exister une interface pour le connecteur AUI (*Attachment Unit Interface*) 15 broches. Utilisé avec l'émetteur-récepteur approprié, ce connecteur permet de raccorder différents médias. En règle générale, un émetteur-récepteur convertit un connecteur AUI en connecteur de type RJ-45, câble coaxial ou fibre optique. Les systèmes 10Base5 Ethernet (ou Thicknet) font appel à un câble court pour relier le connecteur AUI à un émetteur-récepteur sur le câble principal.

La page suivante traite des câbles UTP (câbles à paires torsadées non blindées).

5.1 Câblage des réseaux LAN

5.1.5 Mise en œuvre d'UTP

Cette page comporte des informations détaillées sur la mise en œuvre d'UTP.

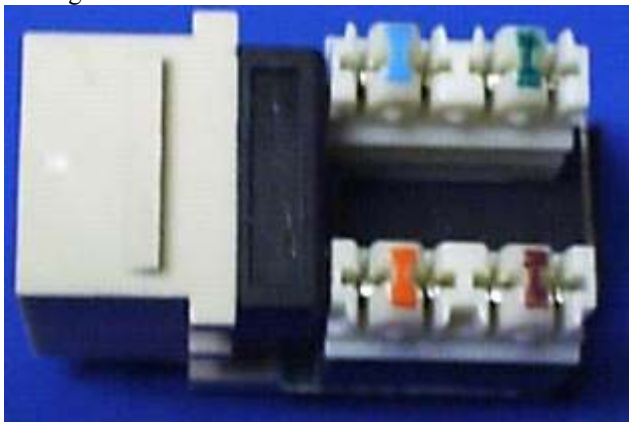


La norme EIA/TIA spécifie un connecteur RJ-45 pour câble UTP. L'acronyme RJ correspond à Registered Jack et le numéro 45 désigne un ordre de connexion des fils spécifique. Le connecteur RJ-45 à extrémités transparentes comporte huit fils de couleur. Quatre de ces fils (T1 à T4), appelés «tips», acheminent la tension. Les quatre autres fils (R1 à R4), ou «rings», sont mis à la terre. Les termes « tip » et « ring » remontent à l'apparition du téléphone. Ils désignent aujourd'hui le fil positif et le fil négatif d'une paire. Les fils de la première paire d'un câble ou d'un connecteur sont appelés T1 et R1. La deuxième paire correspond à T2 et

R2, la troisième à T3 et R3, et la quatrième à T4 et R4.

Le connecteur RJ-45 représente le composant mâle, serti à l'extrémité du câble. Vus de face, les emplacements des broches d'un connecteur mâle sont numérotés de 8 à 1 de la gauche vers la droite, comme l'illustre la figure 1.

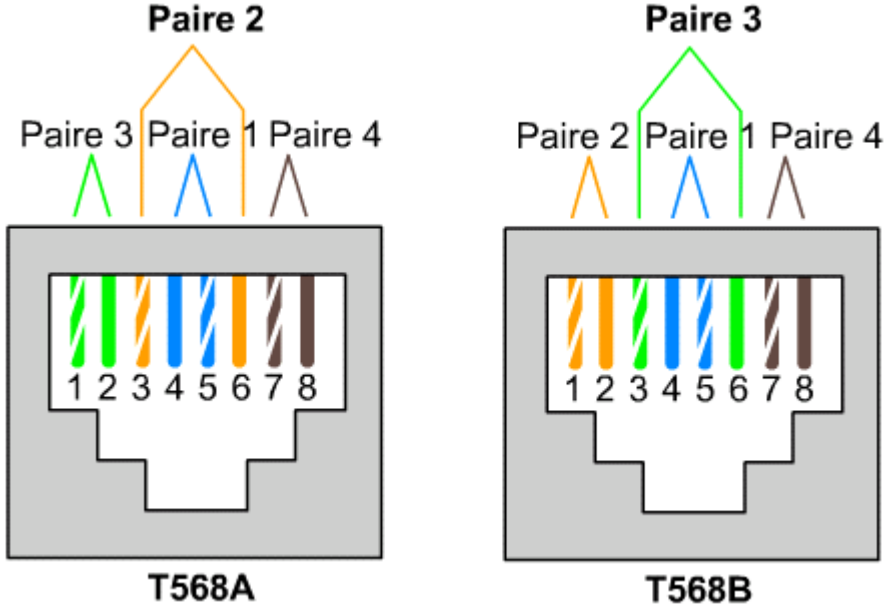
La prise constitue le composant femelle d'un équipement réseau, d'une prise murale ou d'un panneau de brassage, comme l'illustre la figure 2 . La figure 3





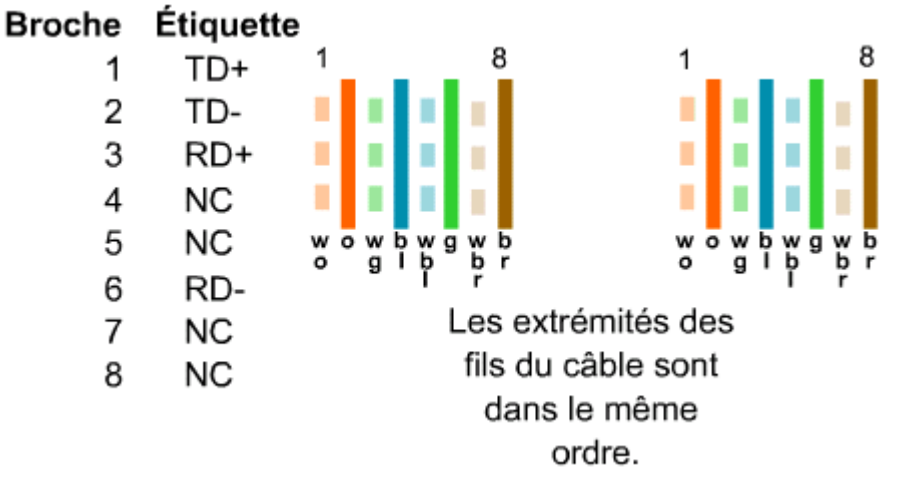
montre les connexions à l'arrière de la prise à laquelle se raccorde le câble UTP Ethernet.

Pour que l'électricité circule entre le connecteur et la prise, l'ordre des fils doit respecter le code de couleurs T568A ou T568B de la norme EIA/TIA-568-B.1, comme le montre la figure 4.



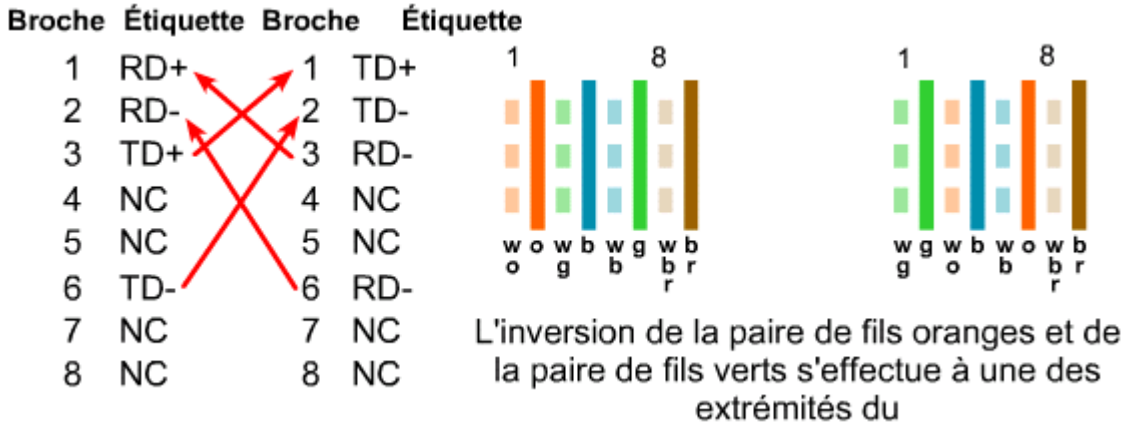
Pour déterminer la catégorie de câble EIA/TIA à utiliser pour raccorder un équipement, consultez la documentation de l'équipement concerné ou recherchez, sur celui-ci, une étiquette proche de la prise. En l'absence d'étiquette et de documentation, utilisez la catégorie 5e ou une catégorie supérieure, les catégories supérieures étant susceptibles de remplacer celles qui leur sont inférieures. Puis, déterminez si vous allez utiliser un câble droit ou un câble croisé.

Si vous maintenez les deux connecteurs RJ-45 d'un câble côte à côte et dans le même sens, vous voyez les fils de couleur dont ils se composent. Si les fils de couleur se présentent dans le même ordre à chaque extrémité, il s'agit d'un câble droit, tel que celui qui est représenté dans la figure 5



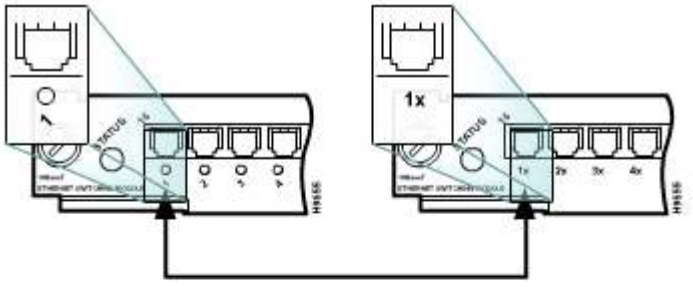
.

Dans le cas d'un câble croisé, certains fils placés aux deux extrémités des connecteurs RJ-45 se raccordent à des broches différentes à chaque extrémité du câble. La figure 6

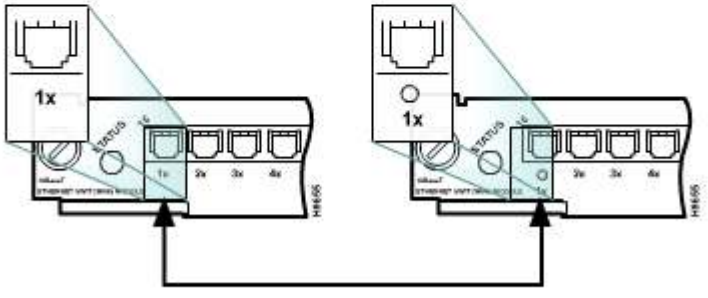

Broche Étiquette Broche Étiquette
1 RD+ 1 TD+
2 RD- 2 TD-
3 TD+ 3 RD-
4 NC 4 NC
5 NC 5 NC
6 TD- 6 RD-
7 NC 7 NC
8 NC 8 NC
1
8
wo o wg b wb g wb r br
1
8
wg g wo b wb o wb r br
L'inversion de la paire de fils oranges et de la paire de fils verts s'effectue à une des extrémités du

montre que les broches 1 et 2 d'un connecteur se raccordent aux broches 3 et 6 de l'autre.

La figure 7



Utilisez un câble droit seulement lorsqu'un port est désigné par un



Utilisez un câble croisé lorsque les DEUX ports sont désignés par un " x " ou lorsque aucun des ports ne présente cette désignation.

illustre les directives qui permettent de déterminer le type de câble à utiliser pour relier les équipements Cisco.

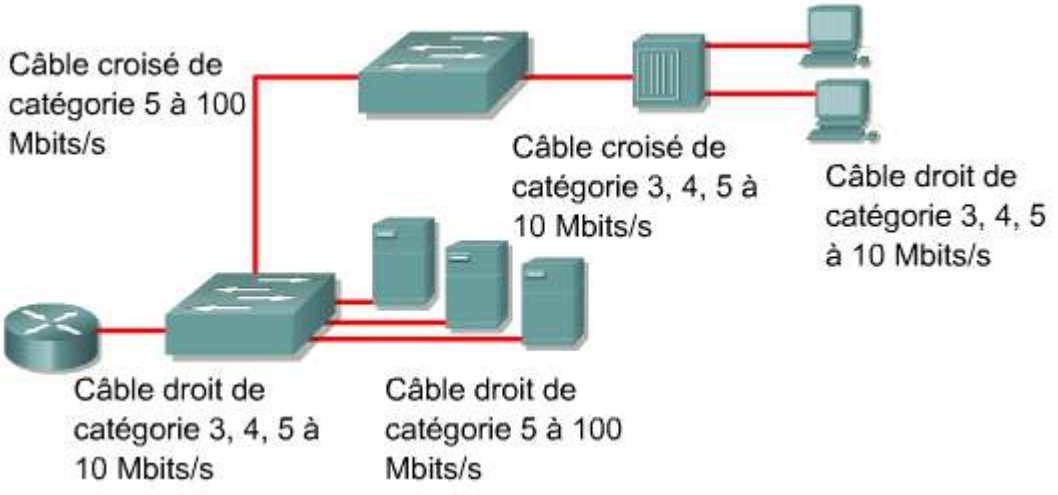
Utilisez des câbles droits pour les liaisons suivantes:

- Commutateur vers routeur
- Commutateur vers PC ou serveur
- Concentrateur vers PC ou serveur

Utilisez des câbles croisés pour les liaisons suivantes:

- Commutateur vers commutateur
- Commutateur vers concentrateur
- Concentrateur vers concentrateur
- Routeur vers routeur
- PC vers PC
- Routeur vers PC

La figure 8


Câble croisé de catégorie 5 à 100 Mbits/s
Câble croisé de catégorie 3, 4, 5 à 10 Mbits/s
Câble droit de catégorie 3, 4, 5 à 10 Mbits/s
Câble droit de catégorie 3, 4, 5 à 10 Mbits/s
Câble droit de catégorie 5 à 100 Mbits/s

montre qu'un réseau donné peut nécessiter plusieurs types de câbles. La catégorie de câble UTP à utiliser dépend du type d'interface Ethernet adopté.

L'activité de TP illustre le processus de raccordement d'une prise RJ-45.

Les activités de média interactives proposent des vues détaillées d'un câble droit et d'un câble croisé.

La page suivante traite du fonctionnement des répéteurs.

Activité de TP

Exercice: Connexions de la prise RJ-45

Ce TP est consacré au processus de raccordement d'une prise RJ-45, ainsi qu'à la procédure d'installation de la prise dans une plaque murale.

Activité de média interactive

Agrandissement: Câble droit

Dans cette vue agrandie, l'étudiant peut observer un câble droit.

Activité de média interactive

Agrandissement: Câble croisé

Dans cette vue agrandie, l'étudiant peut observer un câble croisé.

5.1 Câblage des réseaux LAN

5.1.6 Répéteurs

Cette page traite du mode d'utilisation d'un répéteur sur un réseau.

Le terme «répéteur» remonte à l'origine de la communication longue distance. Le répéteur était une personne, sur une colline, qui répétait le signal qu'elle venait de recevoir d'une autre personne sur la colline précédente. Ce processus se poursuivait jusqu'à ce que le message atteigne sa destination. Les technologies de communication par télégraphe, téléphone, micro-ondes et fibre optique font appel à des répéteurs pour renforcer les signaux envoyés sur de longues distances.

Un répéteur reçoit un signal, le régénère et le transmet. Il peut régénérer les signaux réseau et les resynchroniser au niveau du bit pour leur permettre de voyager sur de plus longues distances via le média. 1 (voir page 47)Les normes Ethernet et IEEE 802.3 mettent en œuvre la règle 5-4-3 relative au nombre de répéteurs et de segments sur les backbones Ethernet à accès partagé dans une topologie arborescente. La règle 5-4-3 divise le réseau en deux types de segments physiques : les segments (utilisateur) avec stations de travail et les segments (de liaison) sans stations de travail. Les systèmes des utilisateurs sont connectés aux segments utilisateur. Les répéteurs du réseau sont reliés entre eux via les segments de liaison. La règle stipule qu'entre deux nœuds du réseau, il ne peut exister que cinq segments au maximum, reliés par le biais de quatre répéteurs (ou concentrateurs), et que seuls trois des cinq segments peuvent contenir des connexions utilisateur.

Dans le cadre du protocole Ethernet, un signal envoyé sur le LAN doit atteindre chaque partie du réseau dans un laps de temps déterminé. La règle 5-4-3 assure le respect de ce principe. Chaque répéteur traversé par un signal ajoute un court intervalle de temps au processus, la règle étant conçue pour limiter les temps de transmission des signaux. Une latence trop importante sur le LAN accroît le nombre de collisions tardives et altère les performances du réseau.

La page suivante traite des concentrateurs.

5.1 Câblage des réseaux LAN

5.1.7 Concentrateurs

Cette page décrit les trois types de concentrateurs.

Les concentrateurs (Hub) sont, en fait, des répéteurs multiports. La différence entre un concentrateur et un répéteur réside dans le nombre de ports respectifs de ces équipements. Un répéteur classique possède généralement deux ports et un concentrateur entre 4 et 24 ports. 1



Les concentrateurs sont couramment utilisés dans les réseaux Ethernet 10BaseT et 100BaseT.

L'utilisation d'un concentrateur modifie la topologie du réseau. La topologie en bus linéaire (chaque équipement est connecté directement au câble) est remplacée par une topologie en étoile. Chaque donnée qui arrive sur le port d'un concentrateur par l'intermédiaire des câbles est électriquement répétée sur tous les autres ports connectés au segment de réseau.

Il existe trois principaux types de concentrateurs:

- **Passif:** un concentrateur passif sert uniquement de point de connexion physique. Il ne peut ni manipuler ni visualiser le trafic acheminé par son intermédiaire. De même, il n'amplifie pas le signal et ne le nettoie pas. Un concentrateur passif permet uniquement de partager le média physique. Il n'a besoin d'aucune alimentation électrique.
- **Actif:** un concentrateur actif doit être branché à une prise de courant pour pouvoir amplifier un signal avant de l'envoyer aux autres ports.
- **Intelligent:** les concentrateurs intelligents (ou «smart hubs») fonctionnent de la même façon que les concentrateurs actifs, avec des puces microprocesseur et des fonctions de diagnostic. Les concentrateurs intelligents sont plus onéreux que les concentrateurs actifs. Ils sont également plus efficaces dans les situations de dépannage.

Les équipements raccordés à un concentrateur reçoivent tout le trafic qui traverse le concentrateur. Plus le nombre d'équipements reliés au concentrateur est important, plus le risque de collisions est élevé. Une collision se produit lorsque plusieurs stations de travail envoient simultanément des données via les câbles du réseau. Dans ce cas, toutes les données sont altérées. Tous les équipements connectés à un segment donné du réseau sont membres du même domaine de collision.

Les concentrateurs, comme leur nom l'indique, constituent des points de connexion centraux pour les réseaux LAN Ethernet.

L'activité de TP vise à enseigner aux étudiants le prix des différents composants réseau.

La page suivante traite des réseaux sans fil.



Activité de TP

Exercice: Achat de concentrateurs et de cartes réseau

Ce TP présente les différents composants réseau disponibles ainsi que leur prix sur le marché.

5.1 Câblage des réseaux LAN

5.1.8 Technologie sans fil

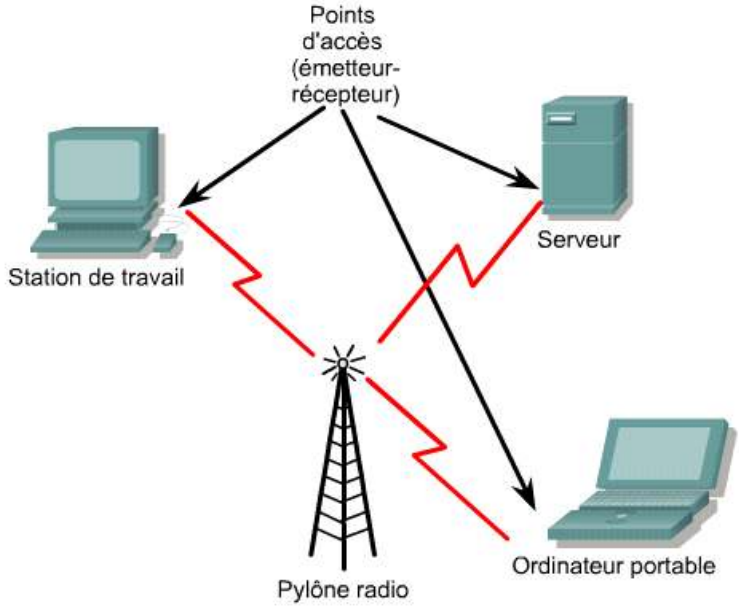
Cette page décrit la création d'un réseau sans fil (wireless network), impliquant un câblage beaucoup moins important que les autres types de réseau.

Les signaux sans fil sont des ondes électromagnétiques qui circulent dans l'air. Les réseaux sans fil utilisent la radiofréquence (RF), des rayons laser, des ondes infrarouges (IR), un satellite ou des micro-ondes pour transporter les signaux entre les ordinateurs sans connexion de câble permanente. Seuls les points d'accès du réseau peuvent faire l'objet d'un câblage permanent. Il devient alors inutile de brancher et débrancher les câbles du réseau pour déplacer les stations de travail membres du réseau sans fil.

La communication avec les mobiles est l'application la plus courante de la transmission de données sans fil. Les aéronefs, les avions, les satellites, les sondes spatiales lointaines, les navettes et les stations spatiales en sont des exemples.

La communication sans fil s'appuie sur des équipements appelés «émetteurs» et «récepteurs». L'émetteur convertit les données source en ondes électromagnétiques, qu'il envoie au récepteur. Puis, le récepteur reconvertit ces ondes électromagnétiques en données pour les envoyer à la destination. Dans le cadre de la communication bidirectionnelle, chaque équipement nécessite un émetteur et un récepteur. La plupart des

fabricants d'équipements réseau intègrent l'émetteur et le récepteur dans une même unité appelée «émetteur-récepteur» (transceiver) ou «carte réseau sans fil». 1



Tous les équipements d'un réseau WLAN doivent être équipés de la carte réseau sans fil appropriée.

Les technologies sans fil IR et RF sont les plus répandues dans le domaine des réseaux. La technologie IR présente toutefois des points faibles. En effet, l'émetteur doit disposer d'une visibilité directe des stations de travail et des équipements numériques pour fonctionner correctement. L'utilisation d'un réseau de type infrarouge implique que tous les équipements numériques nécessitant une connectivité réseau se trouvent dans la même pièce. La technologie réseau IR s'installe rapidement. Cependant, les signaux de données peuvent être affaiblis ou masqués par les personnes qui traversent la pièce ou par l'humidité ambiante. Les nouvelles technologies IR seront à même de fonctionner sans visibilité directe.

La technologie RF permet de placer les équipements dans des pièces ou des bâtiments distincts. La plage limitée de signaux radio restreint l'utilisation de ce type de réseau. Cette technologie peut utiliser une ou plusieurs fréquences. Une fréquence radio unique est sensible aux interférences externes et aux obstructions géographiques. Par ailleurs, elle peut facilement être surveillée par des tiers, ce qui nuit à la sécurité des transmissions de données. L'étalement du spectre utilise plusieurs fréquences pour accroître l'immunité au bruit et éviter que des tiers n'interceptent les transmissions de données.

La mise en œuvre de l'étalement du spectre pour les transmissions WLAN peut s'effectuer selon l'approche FHSS (*Frequency Hopping Spread Spectrum* ou *étalement du spectre à sauts de fréquence*) ou DSSS (*Direct Sequence Spread Spectrum* ou *étalement du spectre en séquence directe*). Les détails techniques liés au fonctionnement de ces technologies ne seront pas abordés dans le cadre de ce cours.

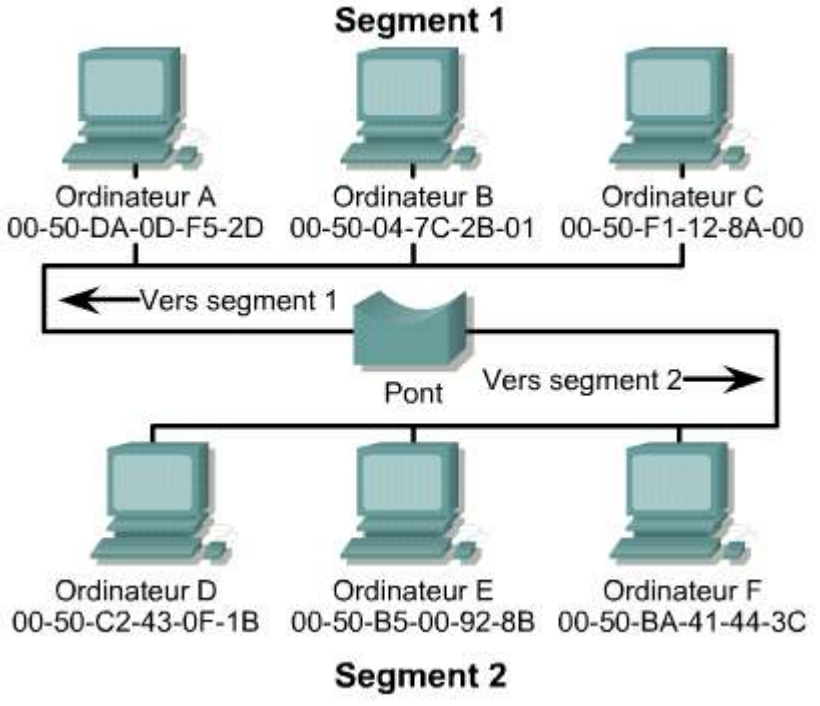
Un réseau LAN de taille importante peut être divisé en plusieurs petits segments. La page suivante explique l'utilisation des ponts à cette fin.

5.1 Câblage des réseaux LAN

5.1.9 Ponts

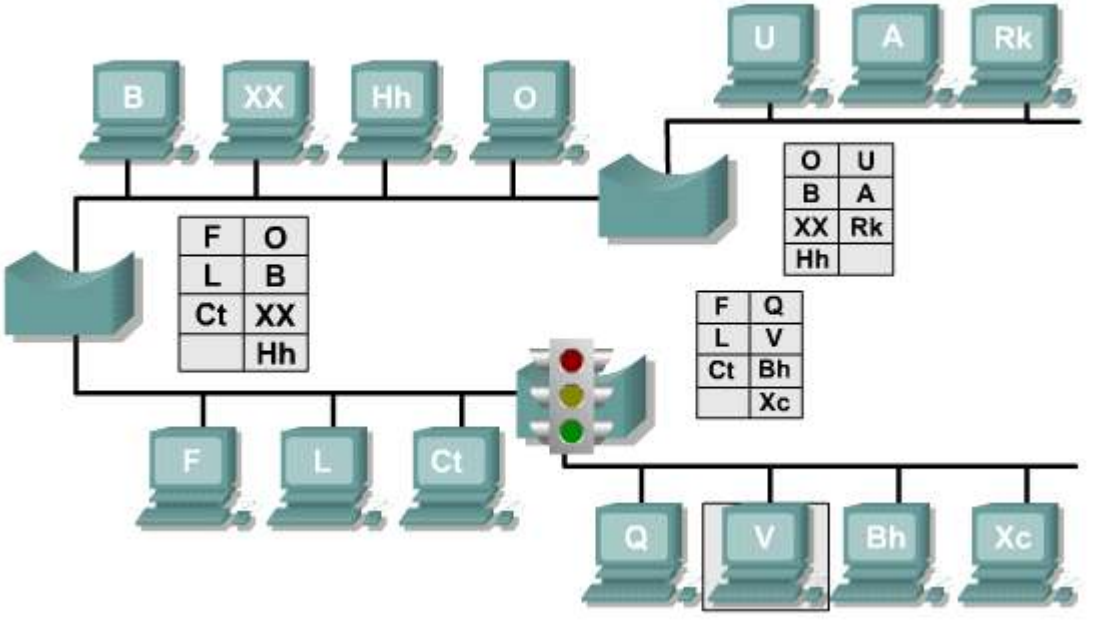
Cette page décrit la fonction des ponts (bridge) dans un réseau LAN.

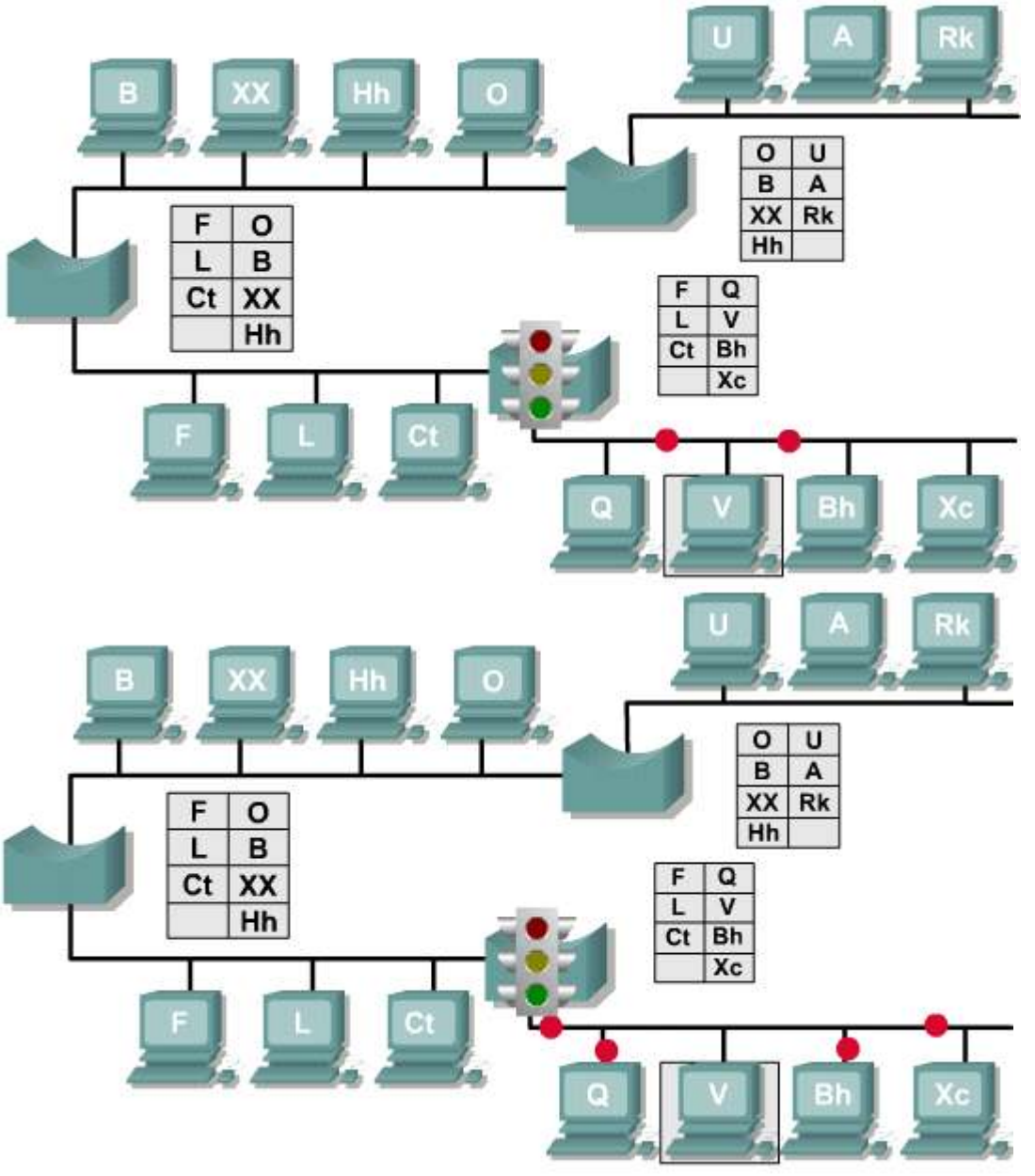
Dans certains cas, il peut s'avérer nécessaire de diviser un LAN de taille importante en plusieurs petits segments, qui seront plus faciles à gérer. 1

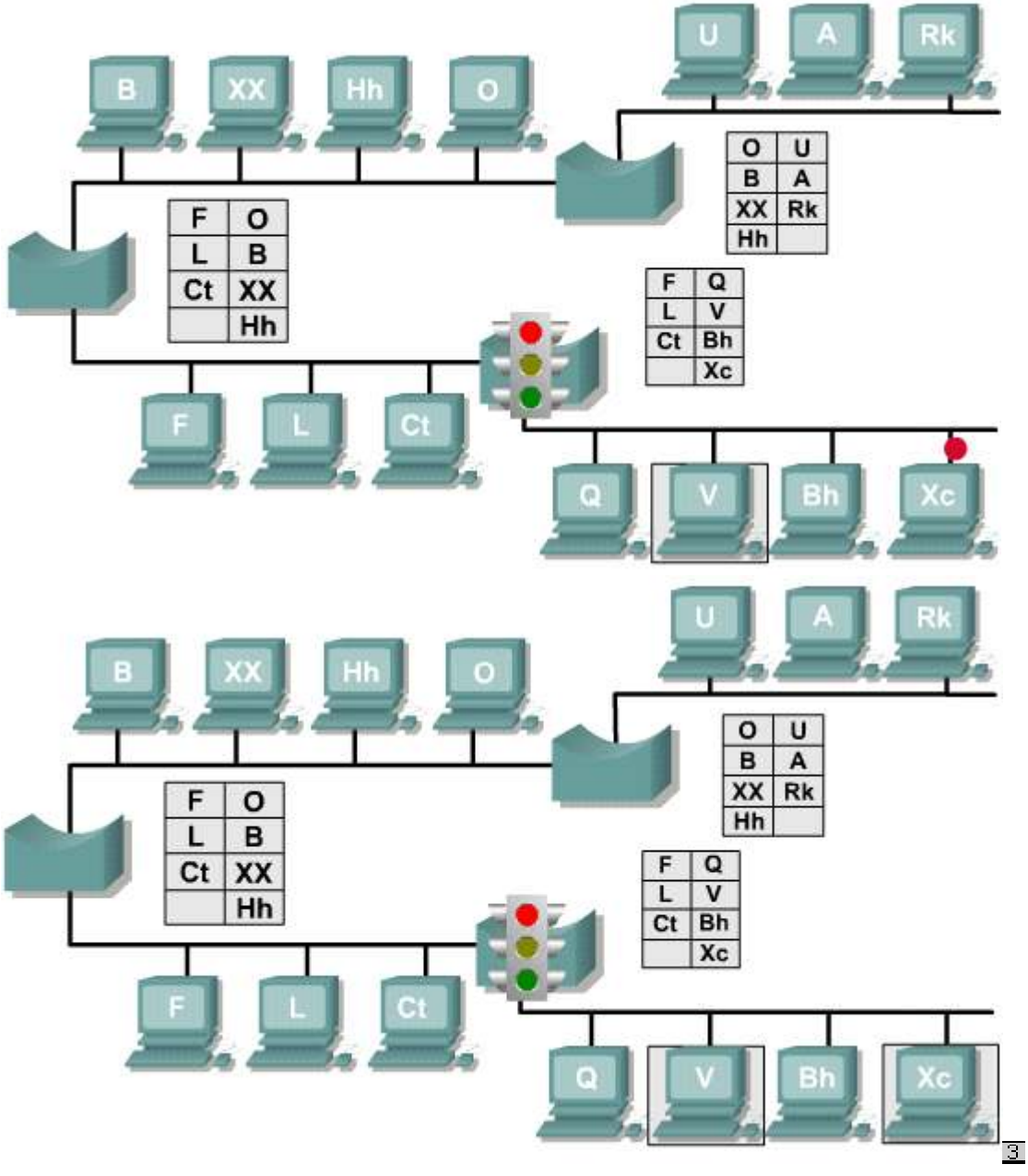


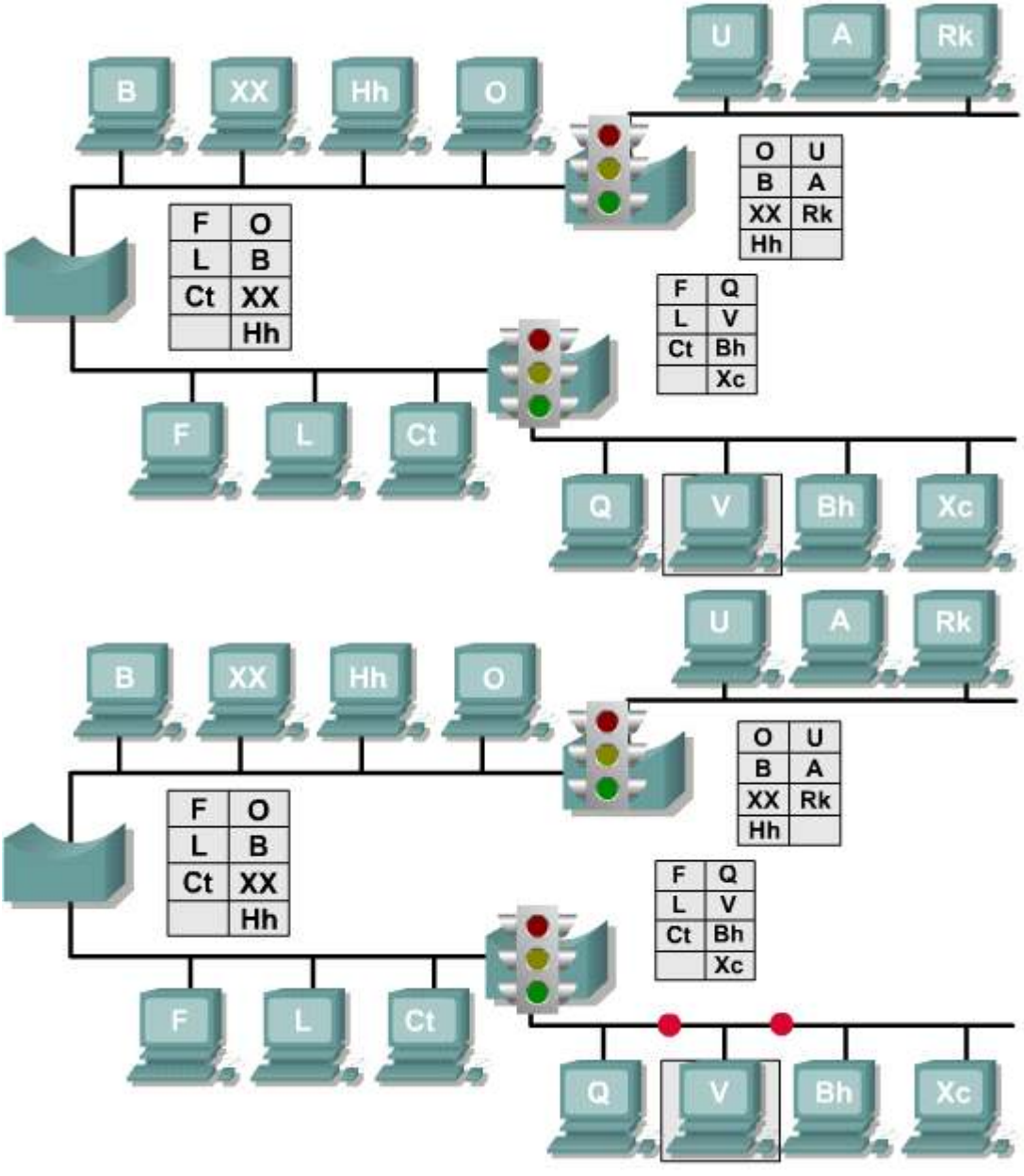
Ceci entraîne la diminution du trafic sur un LAN donné tout en permettant d'étendre la zone géographique précédemment prise en charge par un LAN unique. Vous pouvez utiliser des équipements de type ponts, commutateurs, routeurs et passerelles pour relier les segments du réseau les uns aux autres. Les commutateurs et les ponts fonctionnent au niveau de la couche liaison de données du modèle OSI. Un pont doit prendre des décisions intelligentes quant à la transmission ou non des signaux au segment suivant d'un réseau.

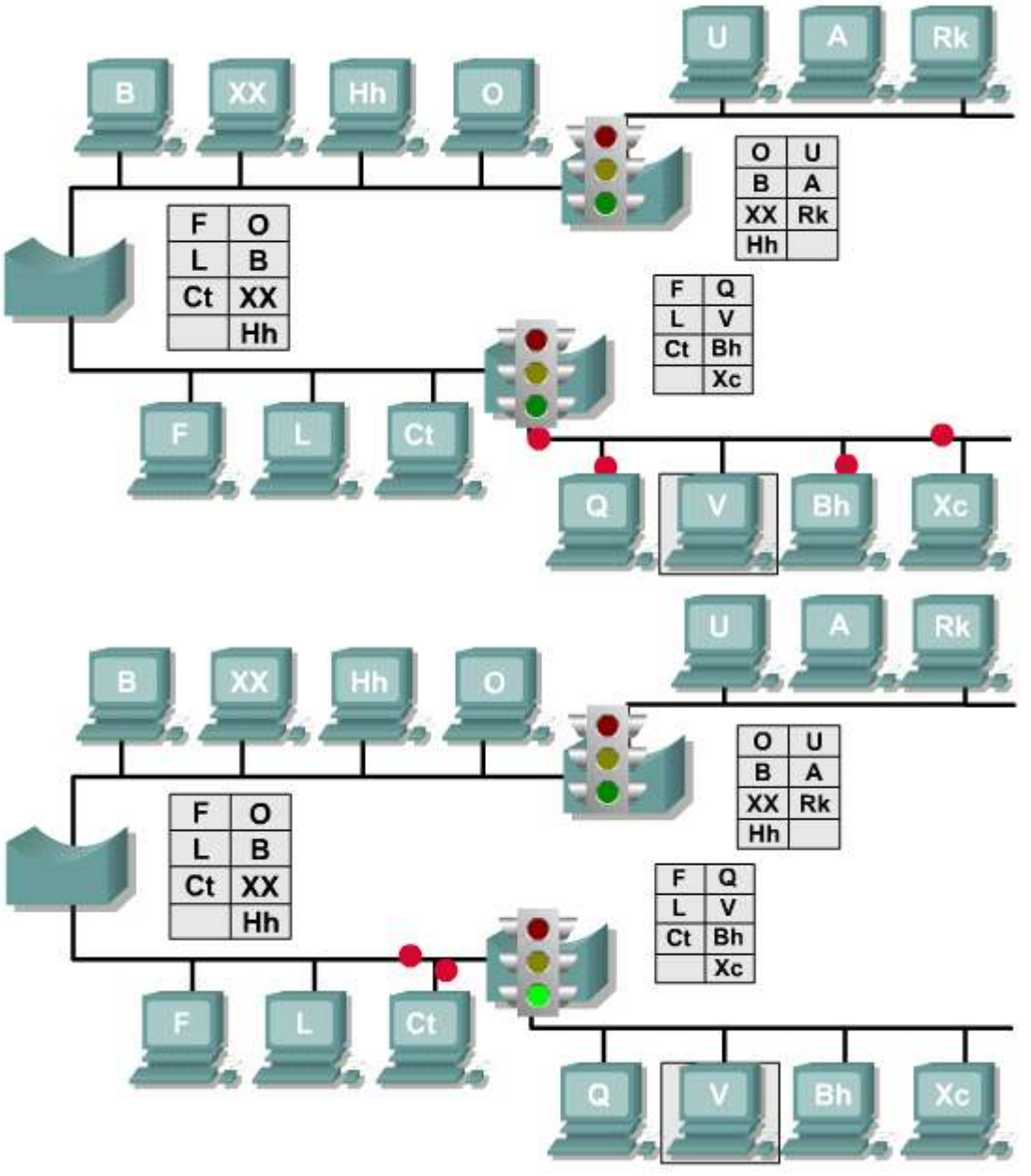
Lorsqu'un pont reçoit une trame sur le réseau, il recherche l'adresse MAC de destination dans une table spécifique afin de déterminer s'il doit filtrer la trame, la diffuser ou la copier sur un autre segment. Ce processus de décision s'effectue comme suit: 2

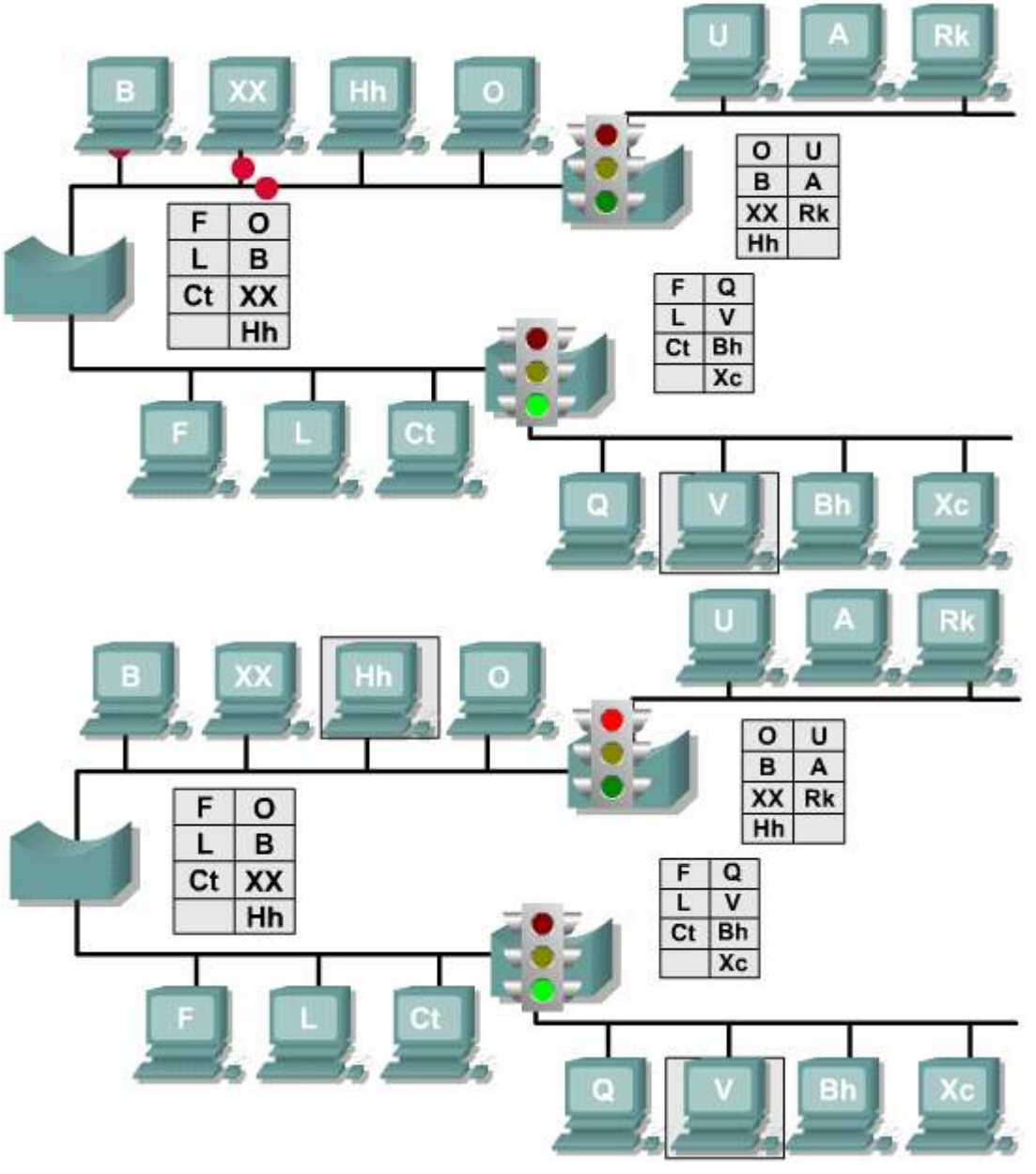



U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc
U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc


U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc
U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc


U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc
U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc


U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc
U
A
Rk
B
XX
Hh
O
O U
B A
XX Rk
Hh
F O
L B
Ct XX
Hh
F Q
L V
Ct Bh
Xc
F
L
Ct
Q
V
Bh
Xc



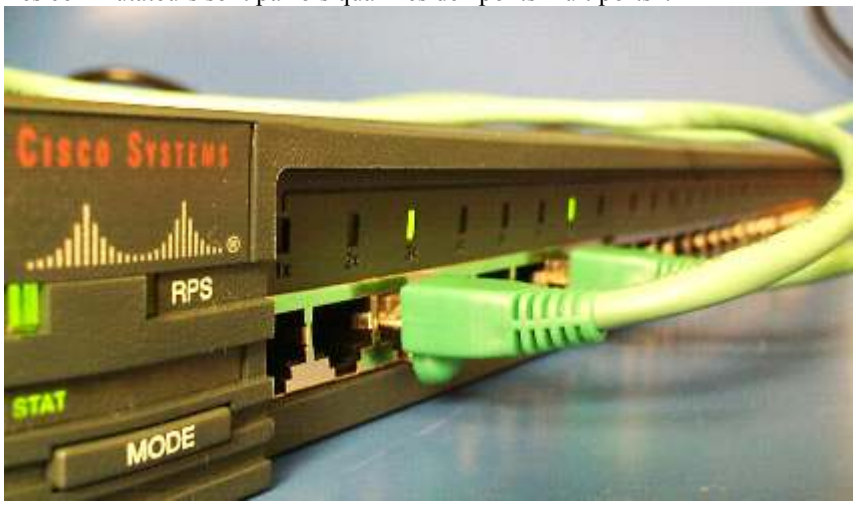
- Si l'équipement de destination se trouve sur le même segment que la trame, le pont n'envoie pas la trame vers d'autres segments. Ce processus correspond au «filtrage».
- Si l'équipement de destination se trouve sur un autre segment, le pont transmet la trame au segment approprié.
- Si le pont ne connaît pas l'adresse de destination, il transmet la trame à tous les segments, excepté à celui par lequel la trame a été reçue. Ce processus correspond à la «diffusion».

Placé de façon stratégique, un pont améliore considérablement les performances réseau.

La page suivante traite des commutateurs.

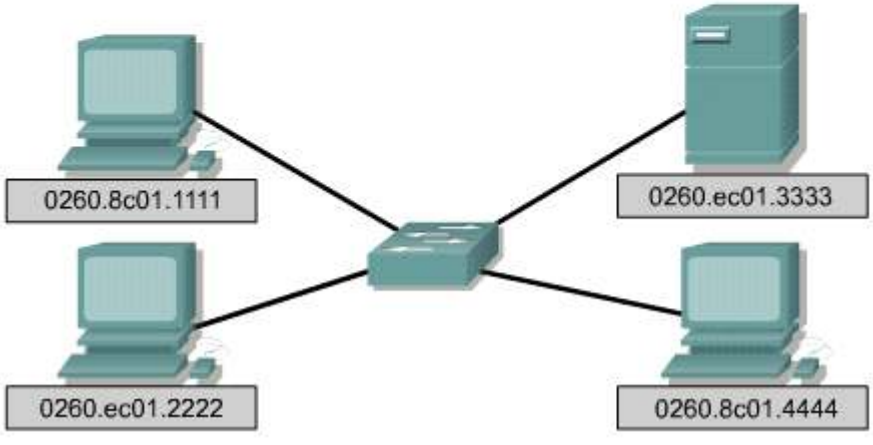
Cette page traite de la fonction des commutateurs (switches).

Les commutateurs sont parfois qualifiés de «ponts multiports». 1

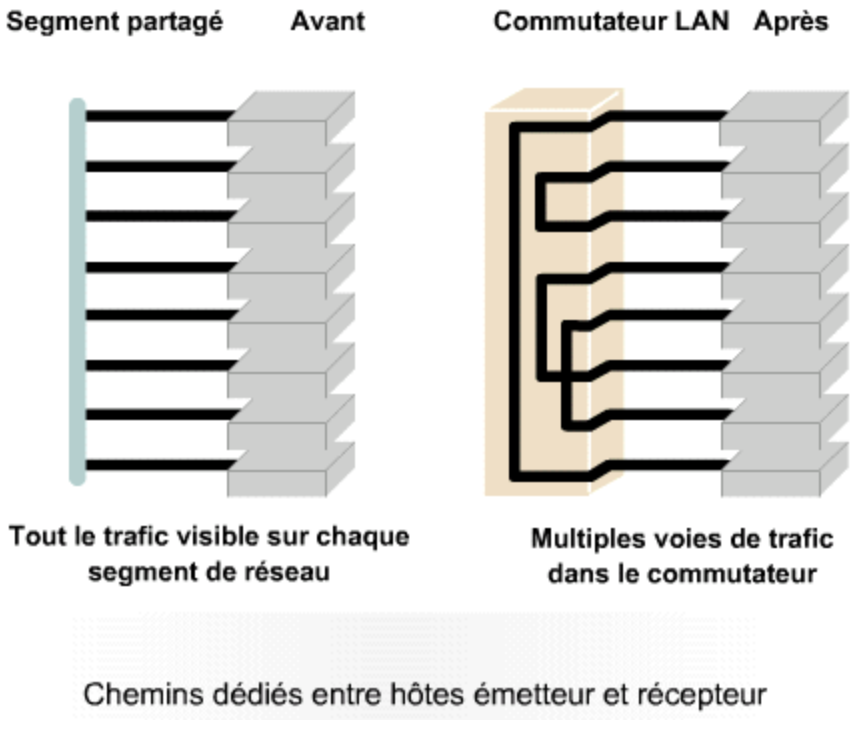


Un pont classique comporte seulement deux ports qui relient deux segments du réseau. Un commutateur peut avoir plusieurs ports, selon le nombre de segments à relier. À l'instar des ponts, les commutateurs recherchent des informations sur les trames de données qu'ils reçoivent de la part des ordinateurs du réseau. Ils se servent ensuite de ces informations pour créer des tables et déterminer la destination des données que s'envoient les ordinateurs sur le réseau. 2

Interface	Adresse MAC
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444



Bien que ces deux équipements présentent des points communs, un commutateur est plus sophistiqué qu'un pont. Un pont s'appuie sur l'adresse MAC de destination pour déterminer si la trame doit être transmise à un autre segment du réseau. Un commutateur possède plusieurs ports auxquels sont reliés plusieurs segments du réseau. Il sélectionne le port auquel est connecté(e) la station de travail ou l'équipement de destination. Les commutateurs Ethernet représentent des solutions de connectivité populaires car ils optimisent la vitesse, la bande passante et les performances du réseau.


Segment partagé
Avant
Commutateur LAN
Après
Tout le trafic visible sur chaque segment de réseau
Multiples voies de trafic dans le commutateur
Chemins dédiés entre hôtes émetteur et récepteur

La commutation est une technologie qui permet d'atténuer la congestion dans les LAN Ethernet en réduisant le trafic et en augmentant la bande passante. Les commutateurs peuvent facilement remplacer les concentrateurs car ils fonctionnent via les infrastructures de câblage existantes. Ceci permet d'améliorer les performances et ne nécessite que des modifications minimes du réseau.

Une unité de commutation exécute deux fonctions de base : la première est la commutation des trames de données. Il s'agit du processus par lequel une trame arrive sur un média d'entrée pour être ensuite transmise à un média de sortie. La seconde est la gestion des fonctions de commutation : les commutateurs créent et gèrent des tables de commutation et recherchent des boucles.

Les commutateurs fonctionnent à des débits beaucoup plus élevés que les ponts et peuvent accepter de nouvelles fonctionnalités, telles que les LAN virtuels (VLAN).

Les commutateurs Ethernet présentent de nombreux avantages. Ils permettent notamment à de nombreux utilisateurs de communiquer en parallèle via l'utilisation de circuits virtuels et de segments réseau dédiés, dans un environnement exempt de toute collision. La bande passante disponible sur le média partagé s'en trouve optimisée. Par ailleurs, un environnement LAN commuté s'avère très économique car il permet de réutiliser le matériel et le câblage existants.

L'activité de TP vise à enseigner aux étudiants le prix d'un commutateur LAN.

La page suivante traite des cartes réseau.

Activité de TP

Exercice: Achat de commutateurs LAN

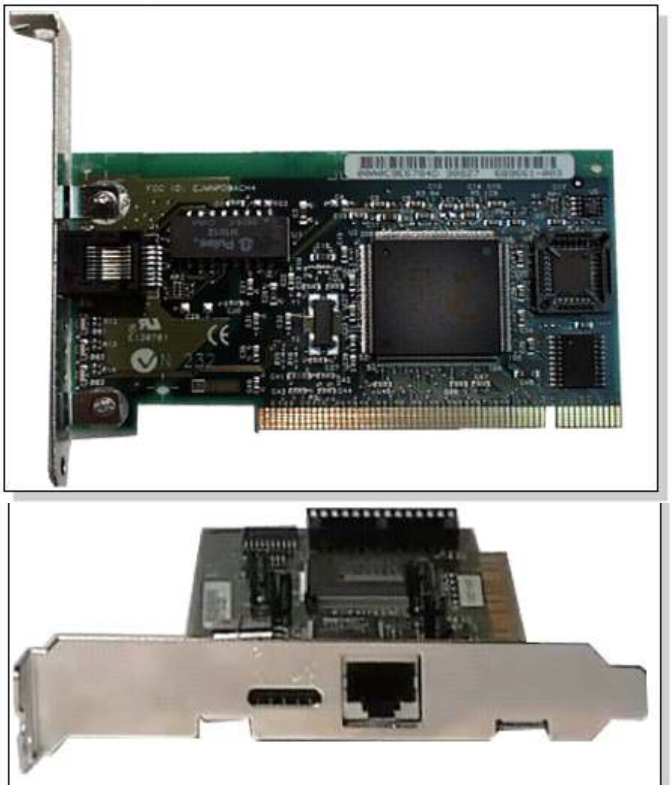
Ce TP présente les différents composants réseau disponibles ainsi que leur prix sur le marché.

5.1 Câblage des réseaux LAN

5.1.11 Connectivité des hôtes

Cette page décrit l'utilisation des cartes réseau pour la mise en œuvre de la connectivité réseau.

Une carte réseau permet de connecter un équipement hôte au média réseau. Il s'agit d'une carte de circuits imprimés qui se loge dans l'emplacement d'extension de la carte mère ou d'un périphérique d'ordinateur. 1 2



La carte réseau est également appelée «adaptateur réseau». Sur les ordinateurs portables, une carte réseau a la taille d'une carte de crédit.

Les cartes réseau sont des équipements de couche 2 car chacune d'entre elles porte un code unique appelé «adresse MAC». Cette adresse permet de contrôler la communication des données de l'hôte sur le réseau. Ce sujet est traité en détail, plus loin dans le cours. Les cartes réseau contrôlent l'accès des hôtes au média.

Dans certains cas, le type de connecteur de la carte ne correspond pas au type de média auquel elle doit être connectée. Le routeur Cisco 2500 en est un bon exemple. Il possède, en effet, un connecteur AUI. Celui-ci doit être raccordé à un câble Ethernet UTP de catégorie 5. Dans ce cas, il convient d'utiliser un émetteur-récepteur qui convertit un type de signal ou un connecteur en un autre. Un émetteur-récepteur permet, par exemple, de raccorder une interface AUI 15 broches à une prise RJ-45. Il s'agit d'un équipement de couche 1 car il fait uniquement appel aux bits et non aux données d'adresse ou aux protocoles des niveaux supérieurs.

Il n'existe pas de symbole standard pour représenter une carte réseau. Lorsque des équipements réseau sont reliés à des médias réseau, la présence d'une carte réseau ou d'un dispositif équivalent est implicite. Un point sur une carte topologique représente une interface NIC ou un port qui assure la fonction de carte réseau.

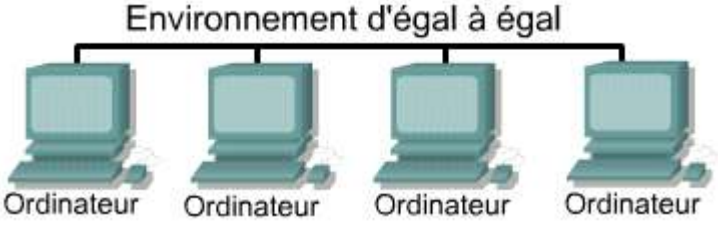
La page suivante traite des réseaux d'égal à égal.

5.1 Câblage des réseaux LAN

5.1.12 Réseaux d'égal à égal

Cette page traite des réseaux d'égal à égal (peer-to-peer).

Dans le cas des technologies LAN et WAN, plusieurs ordinateurs sont reliés entre eux pour proposer des services à leurs utilisateurs. Pour cela, les ordinateurs du réseau assument différents rôles ou fonctions les uns par rapport aux autres. 1

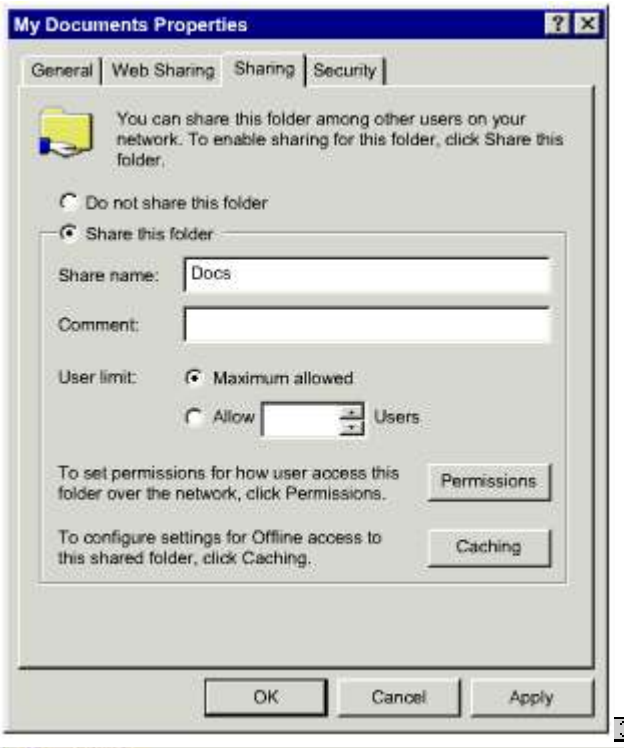


Certains types d'applications exigent que les ordinateurs agissent comme des partenaires égaux. D'autres répartissent leur travail de façon à ce qu'un seul ordinateur en desserve plusieurs dans le cadre d'une relation inégale.

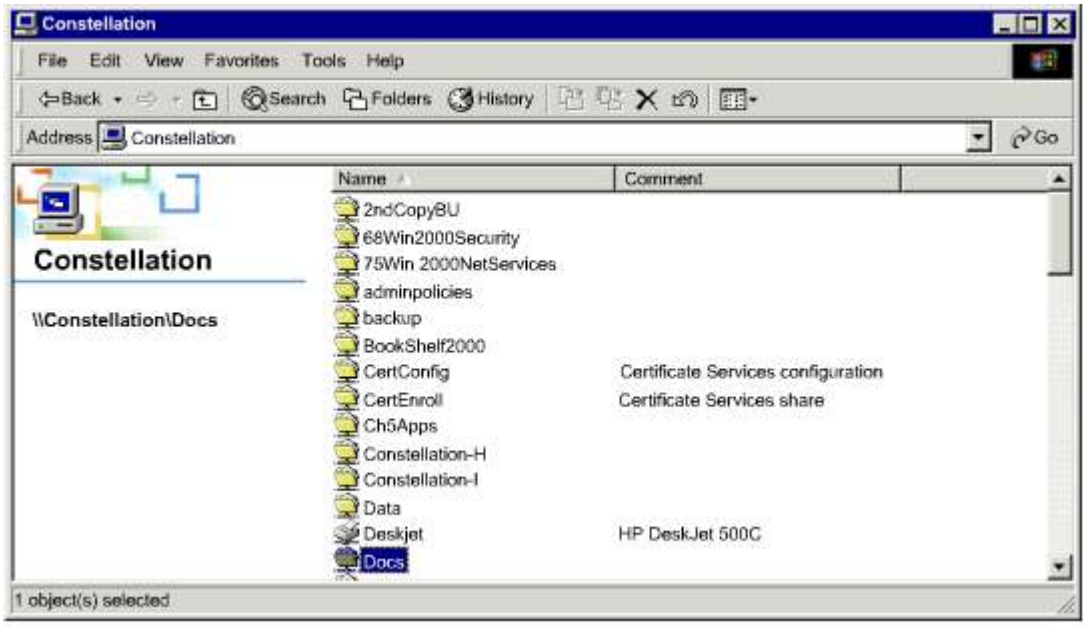
En règle générale, deux ordinateurs communiquent à l'aide de protocoles de requête et de réponse. L'un envoie une requête de service, et l'autre reçoit cette requête et y répond. Le demandeur agit comme un client et son destinataire comme un serveur.

Les ordinateurs membres d'un réseau d'égal à égal se comportent comme des partenaires égaux (ou «pairs»). En tant que pair, chaque ordinateur peut tour à tour assurer la fonction de client et de serveur. Par exemple, l'ordinateur A demande un fichier à l'ordinateur B, qui le lui envoie. L'ordinateur A assure donc la fonction de client et l'ordinateur B celle de serveur. Par la suite, les ordinateurs A et B peuvent inverser leurs fonctions respectives.

Dans un réseau d'égal à égal, chaque utilisateur contrôle ses propres ressources et peut décider de partager certains fichiers avec des tiers. 2



3



Les utilisateurs peuvent, toutefois, demander des mots de passe pour autoriser les tiers à accéder à leurs ressources. Il incombe aux utilisateurs de prendre cette décision car ce type de réseau ne comporte aucun point de contrôle ou d'administration central. Par ailleurs, chaque utilisateur doit sauvegarder son propre système pour pouvoir récupérer les données perdues en cas de panne. Lorsqu'un ordinateur assure la fonction de serveur, son utilisateur peut être confronté à une altération des performances du fait que la machine répond aux requêtes d'autres systèmes.

Les réseaux d'égal à égal sont relativement simples à installer et à utiliser. Aucun équipement supplémentaire n'est nécessaire; il suffit que chaque ordinateur soit équipé d'un système d'exploitation approprié. Les utilisateurs gérant eux-mêmes leurs ressources, aucun administrateur spécialisé ne doit intervenir.

Cependant, l'extension des réseaux accroît la difficulté de coordination des relations d'égal à égal. Ce type de réseau fonctionne bien avec dix ordinateurs au plus. Étant donné le manque d'évolutivité des réseaux d'égal à égal, leur efficacité décroît parallèlement à l'augmentation du nombre d'ordinateurs connectés. Par ailleurs, chaque utilisateur contrôlant l'accès aux ressources de son ordinateur, la sécurité peut être difficile à assurer. Le modèle de réseau client-serveur permet de passer outre les limites du réseau d'égal à égal.

Au cours de l'activité de TP, les étudiants vont créer un réseau d'égal à égal simple.

La page suivante traite d'un réseau client-serveur.

Activité de TP

Exercice: Création d'un réseau d'égal à égal

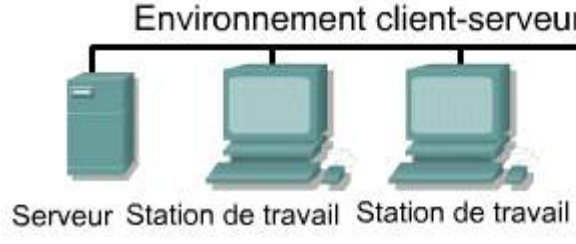
Ce TP porte sur la création d'un réseau d'égal à égal entre deux PC, l'identification du câble approprié pour les relier, la configuration des données d'adresse IP des stations de travail et le test de connectivité via la commande ping.

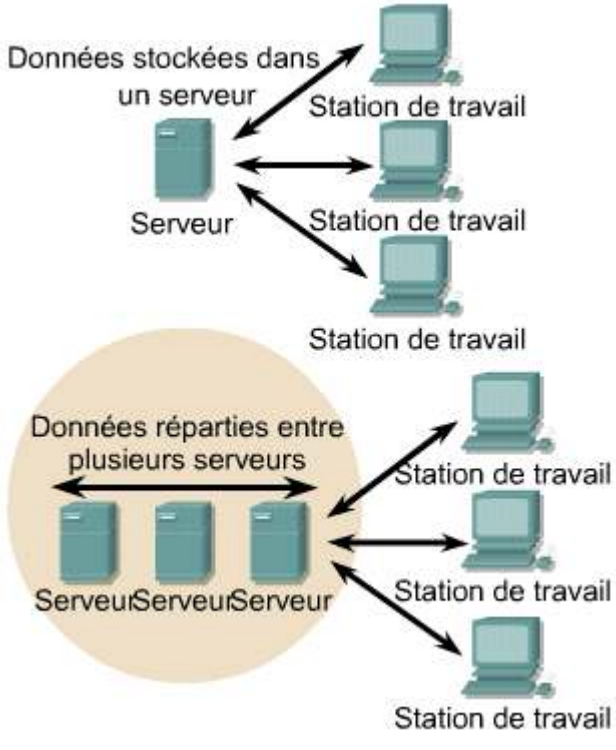
5.1 Câblage des réseaux LAN

5.1.13 Environnement client-serveur

Cette page décrit un environnement client-serveur.

Dans un environnement client-serveur, les services réseau tournent sur un ordinateur dédié appelé « serveur ». Le serveur répond aux requêtes des clients. 1





Il s'agit d'un ordinateur central qui est disponible en permanence pour répondre aux requêtes émises par les clients en matière de services de fichiers, d'impression, d'application ou autres. Nombre de systèmes d'exploitation de réseau adoptent la forme d'une relation client-serveur. En règle générale, les ordinateurs de bureau agissent en tant que clients, alors qu'un ou plusieurs ordinateurs équipés d'un logiciel dédié et dotés d'une puissance de traitement et d'une mémoire plus importantes assurent la fonction de serveurs. 2

Les serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients. Pour qu'un client puisse accéder aux ressources du serveur, il doit être identifié, puis autorisé à utiliser ces ressources. Chaque client possède un nom de compte et un mot

de passe, vérifié par un service d'authentification. Ce service protège l'accès au réseau. En centralisant les comptes utilisateurs, la sécurité et le contrôle d'accès, les environnements client-serveur simplifient l'administration des réseaux de grande taille.

La concentration de ressources réseau, telles que des fichiers, des imprimantes et des applications sur des serveurs facilite également la sauvegarde et la gestion des données. Les ressources peuvent être stockées sur des serveurs dédiés spécialisés pour être plus facilement accessibles. La plupart des systèmes client-serveur offrent également des possibilités d'optimisation du réseau via de nouveaux services destinés à en étendre l'utilité.

L'aspect centralisé des fonctions d'un réseau client-serveur présente des avantages considérables et quelques inconvénients. Bien qu'un serveur centralisé optimise la sécurité, la facilité d'accès et le contrôle, il constitue un point de défaillance unique dans le réseau. En effet, sans un serveur opérationnel, le réseau ne peut plus fonctionner. Par ailleurs, seul un membre de l'équipe expert et formé peut assurer l'administration et la maintenance des serveurs. Cela accroît le coût de fonctionnement du réseau. Les systèmes serveurs nécessitent également du matériel complémentaire et des logiciels spécialisés qui en augmentent le coût.

Les figures 3

Avantages d'un réseau d'égal à égal	Avantages d'un Réseau client-serveur
Implémentation moins coûteuse	Meilleure sécurité
Ne demande pas d'autre logiciel spécialisé dans l'administration réseau	Plus facile à administrer lorsque le réseau est important car l'administration est centralisée.
Ne demande pas d'administrateur réseau dédié.	Possibilité de sauvegarde de toutes les données dans un emplacement central.

et 4

Inconvénients d'un réseau d'égal à égal	Inconvénients d'un réseau client-serveur
Ne s'adapte pas bien aux réseaux importants et complexité de l'administration.	Nécessite un logiciel coûteux, spécialisé pour l'exploitation et l'administration du réseau
Chaque utilisateur doit être formé aux tâches d'administration.	Le serveur nécessite du matériel plus puissant, mais coûteux.
Moins sécurisé	Requires a professional administrator.
Toutes les machines partageant les ressources diminuent les performances	Présente un point de défaillance unique. Indisponibilité des données utilisateur en cas d'arrêt du serveur.

résument les avantages et les inconvénients des réseaux d'égal à égal et client-serveur.

Dans les activités de TP, les étudiants vont créer un réseau à l'aide d'un concentrateur, puis à l'aide d'un commutateur.

Cette page conclut la leçon. La leçon suivante traite du câblage des réseaux WAN. La première page est consacrée à la couche physique des WAN.

Activité de TP

Exercice: Création d'un réseau à l'aide d'un concentrateur

Ce TP porte sur la création d'un réseau simple de deux PC à l'aide d'un concentrateur, l'identification du câble approprié pour relier les PC au concentrateur, la configuration des données d'adresse IP des stations de travail et le test de connectivité via la commande **`ping`**.

5.2 Câblage des réseaux WAN

5.2.1 Couche physique WAN

Cette page présente la couche physique des réseaux WAN.

Les mises en œuvre de couche physique diffèrent selon la distance de l'équipement par rapport à chaque service, la vitesse et le type de service. 1

Cisco HDLC / PPP / Frame Relay	RNIS BRI	Modem DSL	Modem câble
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 HSSI (High Speed Serial Interface)	RJ-45 Remarque : Les broches du câble RNIS BRI sont différentes de celles utilisées pour Ethernet.	RJ-11 Remarque : transmission via une ligne téléphonique	F Remarque : transmission via une ligne de télévision par câble

- La mise en œuvre de couche physique varie.
- Les spécifications de câble définissent la vitesse d'une liaison.

Les services WAN sont pris en charge via des connexions série du type lignes louées spécialisées exécutant PPP ou Frame Relay. Le débit de ces connexions s'étend de 2 400 bits/s à 1 544 Mbits/s pour le service T1 et 2 048 Mbits/s pour le service E1.

La technologie RNIS propose l'établissement de connexions à la demande et des services d'appel de secours par l'infrastructure commutée. Une interface RNIS BRI (*Basic Rate Interface*) se compose de deux canaux Bearer (canaux B) de 64 kbits/s pour les données et d'un canal delta (canal D) de 16 kbits/s utilisé pour la signalisation et d'autres tâches de gestion des liaisons. Le protocole PPP est généralement utilisé pour transporter des données via les canaux B.

Les connexions DSL et modem câble ont gagné en popularité avec l'accroissement de la demande en services de connexion haut débit et à large bande résidentielle. Le service DSL résidentiel type peut atteindre les débits T1/E1 via la ligne téléphonique. Les services modem câble utilisent le câble coaxial de la télévision. Une ligne en câble coaxial offre une connectivité haut débit égale ou supérieure à une connexion DSL. La connexion DSL et le service modem câble seront traités plus en détail dans un autre module.

Les étudiants peuvent identifier les composants de la couche physique du réseau WAN dans l'activité de média interactive.

La page suivante présente les connexions série WAN.

Activité de média interactive

Glisser-Positionner: Mise en œuvre de couche physique WAN

À la fin de cette activité, l'étudiant sera en mesure d'identifier les composants de la couche physique du réseau WAN.

5.2 Câblage des réseaux WAN

5.2.2 Connexions série WAN

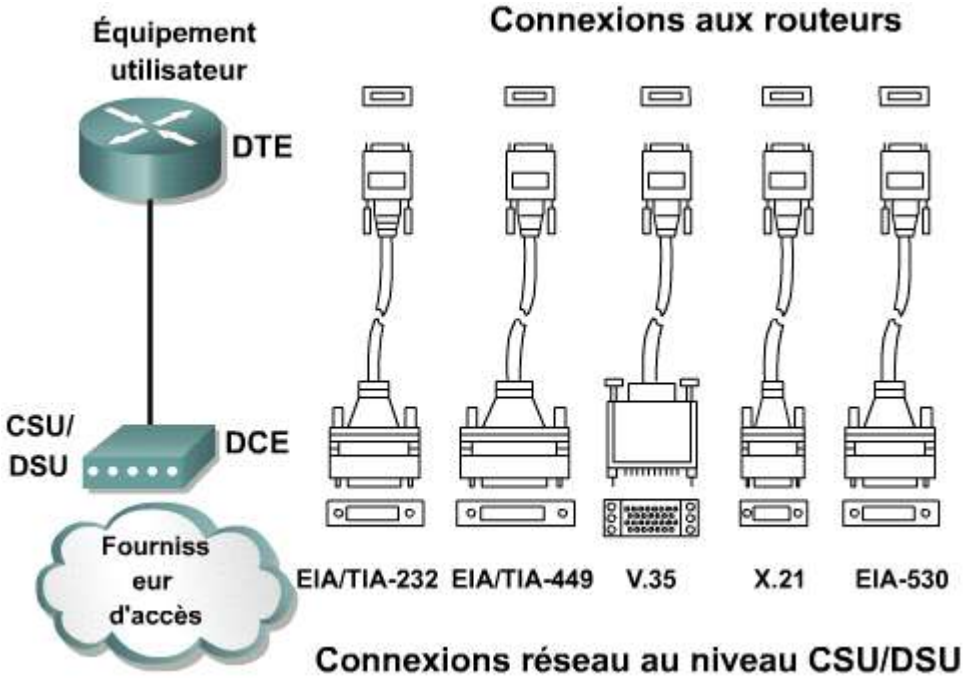
Cette page traite des connexions série WAN.

Pour les communications longue distance, les réseaux WAN font appel à la transmission série. Ce processus consiste envoyer des bits de données via un canal unique. Il accroît la fiabilité des communications longue distance et permet d'utiliser une plage spécifique de fréquences optiques ou électromagnétiques.

Les fréquences se mesurent en cycles par seconde et sont exprimées en hertz (Hz). Les signaux transmis via les lignes téléphoniques à fréquence vocale utilisent 4 kHz. La taille de la plage de fréquences correspond à la bande passante. Dans le domaine des réseaux, la bande passante est la mesure du nombre de bits transmis par seconde. 1

Données (bits/s)	Distance (mètres) EIA/TIA-232	Distance (mètres) EIA/TIA-449
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3.7	—
T1 (1.544 Mbps)	—	15

Pour un routeur Cisco, la connectivité physique sur le site du client est mise en œuvre par le biais d'un ou deux types de connexions série. Le premier type est un connecteur 60 broches et le second un connecteur « série intelligent » plus compact. Le connecteur du fournisseur peut varier selon le type d'équipement de service. 2



Si la connexion s'effectue directement auprès d'un fournisseur de services ou d'un équipement doté d'un signal de synchronisation tel qu'une unité CSU/DSU (*channel service unit/data service unit*), le routeur est alors considéré comme un équipement terminal de traitement de données (ETTD) et utilise un câble série ETTD. Tel est généralement le cas. Toutefois, dans certains cas, le routeur local doit fournir la fréquence d'horloge et utilise donc un câble d'équipement de communication de données ou câble ETCD. Dans les TP sur les routeurs du cursus, l'un des routeurs connectés devra assurer la fonction de synchronisation. La connexion consistera donc en un câble ETTD et un câble ETCD.

La page suivante présente les routeurs et les connexions série.

5.2 Câblage des réseaux WAN

5.2.3 Routeurs et connexions série

Cette page traite de l'utilisation des routeurs et des connexions série dans un réseau WAN.

Les routeurs sont responsables du routage des paquets de données de la source à la destination au niveau du LAN, ainsi que de la connectivité au WAN. Dans l'environnement d'un LAN, le routeur stoppe les broadcasts, fournit les services de résolution d'adresse du type ARP et RARP et peut segmenter le réseau via une structure de sous-réseaux. Pour proposer ces services, le routeur doit être connecté au LAN et au WAN.

Outre le type de câble, il convient de déterminer les connecteurs à utiliser (ETTD ou ETCD). L'ETTD est le point d'extrémité de l'équipement d'un utilisateur au niveau de la liaison WAN. L'ETCD est, en général, le point auquel la responsabilité de la diffusion des données est reportée sur le fournisseur de services.

Lorsque vous vous connectez directement à un fournisseur de services ou à un équipement tel qu'une unité CSU/DSU qui doit exécuter le signal de synchronisation, le routeur constitue un équipement ETTD et doit être

équipé d'un câble série du même type. 1

Équipement terminal de traitement de données :

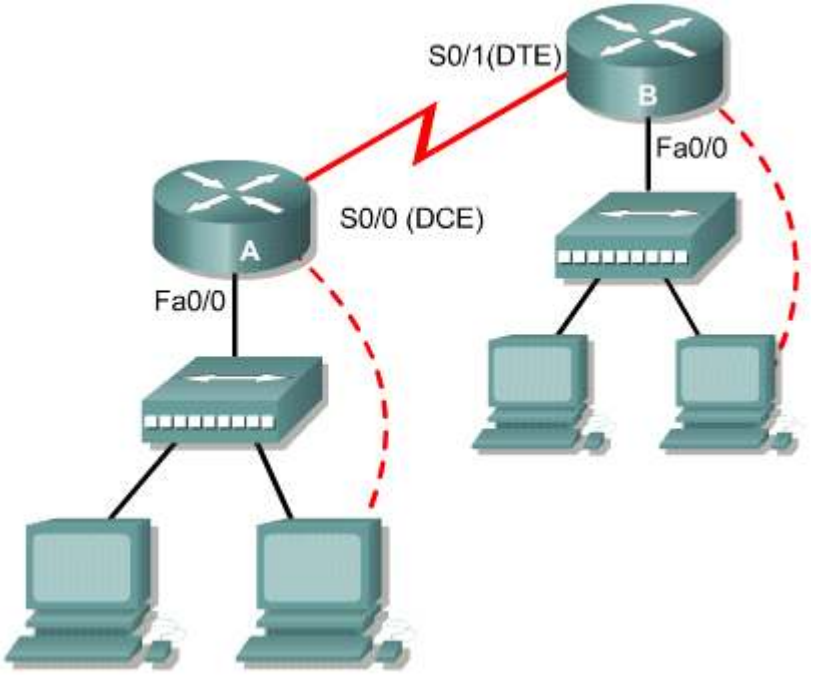
- Extrémité de l'équipement utilisateur sur la liaison WAN

Équipement de communication de données :

- Extrémité du côté du fournisseur d'un réseau WAN côté de l'unité de communication
- Responsable de la synchronisation

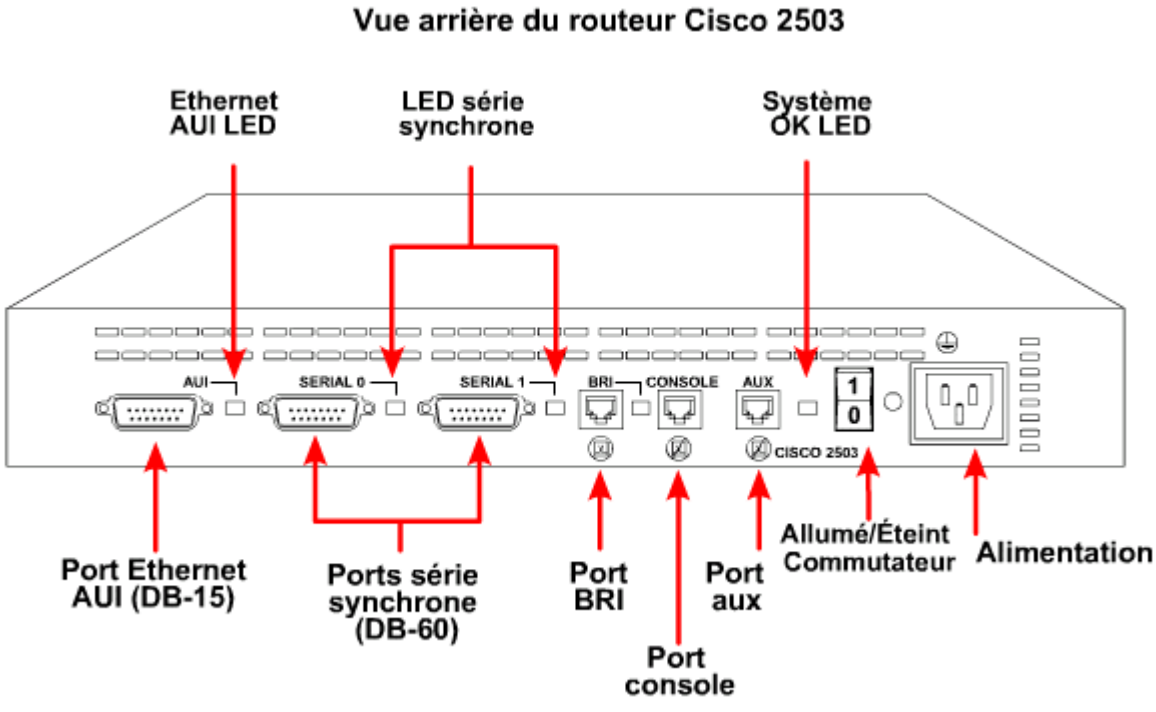


Tel est généralement le cas des routeurs. Cependant, le routeur doit, dans certains cas, être l'équipement ETCD. Lorsque vous exécutez un scénario avec des routeurs dos à dos dans un environnement de test, l'un des routeurs est un équipement ETTD et l'autre un équipement ETCD. 2

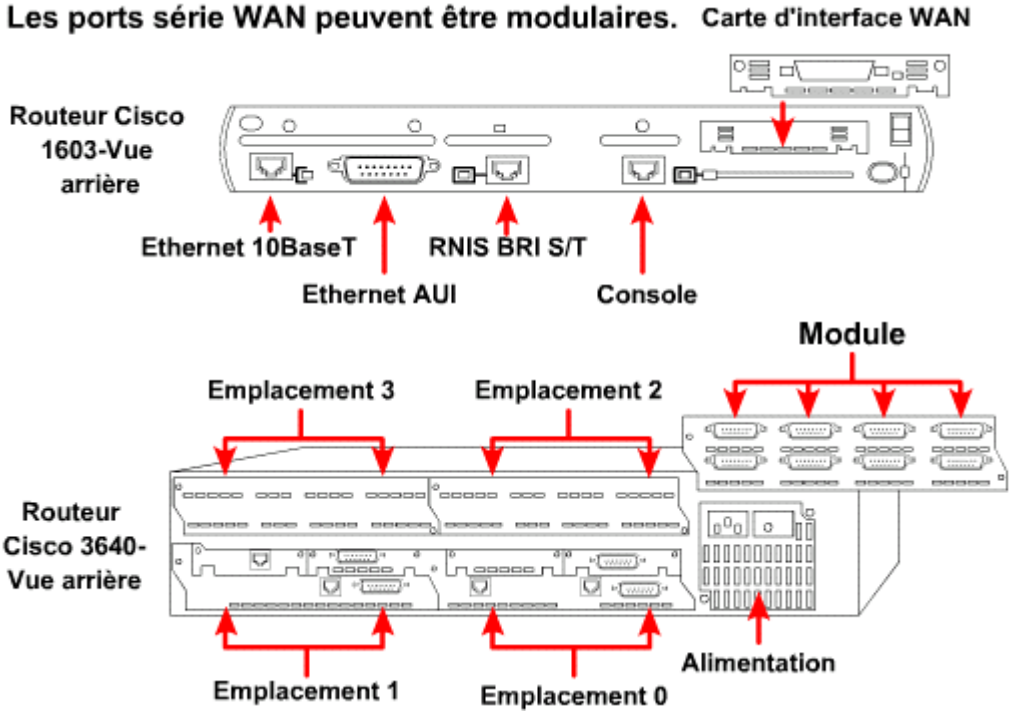


Les routeurs câblés pour une connectivité série peuvent comporter des ports fixes ou modulaires. Le type de port utilisé détermine, par la suite, la syntaxe utilisée pour la configuration des différentes interfaces.

Sur les routeurs dotés de ports série fixes, la dénomination des interfaces doit spécifier le type et le numéro de port. 3



Sur les routeurs équipés de ports série modulaires, la dénomination des interfaces doit indiquer le type de port, l'emplacement et le numéro de port. 4



L'emplacement est le logement du module. Pour configurer un port sur une carte modulaire, il convient de spécifier l'interface à l'aide de la syntaxe «type de port numéro d'emplacement/numéro de port». Utilisez la dénomination "serial 1/0" quand l'interface est une interface série, quand l'emplacement dans lequel est installé le module porte le numéro 1 (slot 1) et quand le port série référencé est le port 0.

Durant la première activité de TP, les étudiants vont identifier les interfaces Ethernet ou Fast Ethernet sur un routeur.

Lors des deux activités suivantes, ils seront amenés à créer et à dépanner un WAN de base.

La page suivante présente les routeurs et les connexions RNIS BRI.

Activité de TP

Exercice: Connexion des interfaces LAN d'un routeur

Ce TP vise à identifier les interfaces Ethernet ou Fast Ethernet sur le routeur.

Activité de TP

Exercice: Création d'un réseau WAN routé de base

Ce TP porte sur la création d'un WAN routé simple comportant deux PC, deux commutateurs ou concentrateurs et deux routeurs.

Activité de TP

Exercice: Dépannage d'équipements interconnectés

Au cours de ce TP, vous serez amené à identifier et à corriger les problèmes réseau liés au câblage et à l'adressage IP des stations de travail.

5.2 Câblage des réseaux WAN

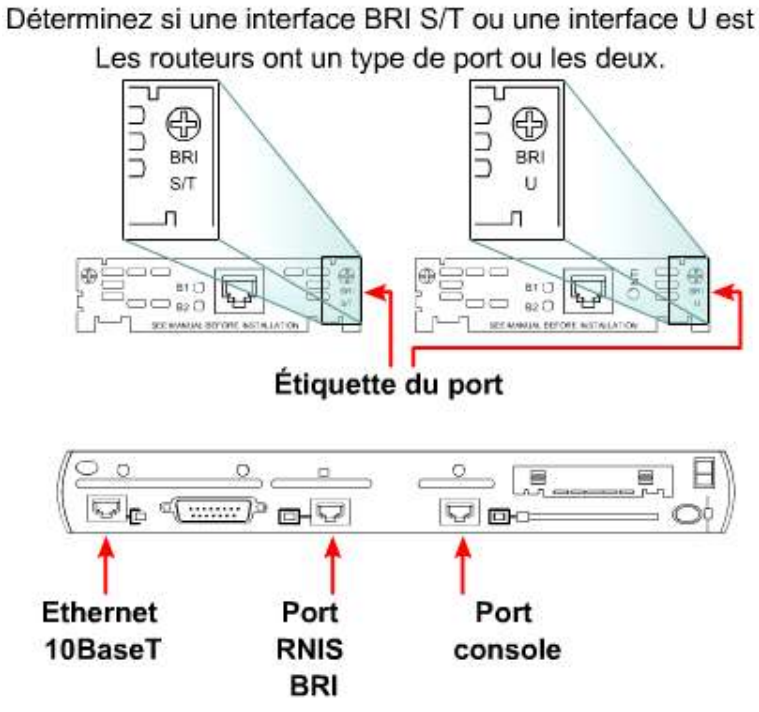
5.2.4 Routeurs et connexions RNIS BRI

Cette page présente en détail les connexions RNIS BRI.

Une connexion RNIS BRI peut faire appel à deux types d'interfaces: BRI S/T et BRI U. Pour déterminer le type d'interface à utiliser, il convient de savoir qui fournit l'équipement de terminaison de réseau 1 (NT1).

Le NT1 est un équipement intermédiaire, situé entre le routeur et le commutateur RNIS de l'opérateur télécom. Cet équipement permet de relier le câblage à quatre fils de l'abonné à la boucle locale traditionnelle à deux fils. En Amérique du Nord, le client fournit généralement l'équipement NT1, ce qui n'est pas le cas dans le reste du monde, où l'opérateur télécom en est responsable.

Il peut s'avérer nécessaire d'ajouter un équipement NT1 externe si celui-ci n'est pas intégré au routeur. L'examen des étiquettes disponibles au niveau des interfaces du routeur permet facilement de déterminer si ce routeur comporte un NT1 intégré. Une interface BRI dotée d'un NT1 intégré est étiquetée «BRI U»; dans le cas contraire, elle présente l'étiquetage «BRI S/T». Il est conseillé de déterminer l'interface nécessaire lors de l'achat car les routeurs peuvent avoir plusieurs types d'interfaces RNIS. L'étiquette du port permet de déterminer le type d'interface BRI. 1



Pour relier le port RNIS BRI à l'équipement de l'opérateur télécom, utilisez un câble droit à paire torsadée non blindée (UTP) de catégorie 5.

ATTENTION: L'extrémité du câble d'un port RNIS BRI ne doit être reliée qu'à une prise ou à un commutateur RNIS. Les connexions RNIS BRI utilisent des tensions qui peuvent gravement endommager les équipements non-RNIS.

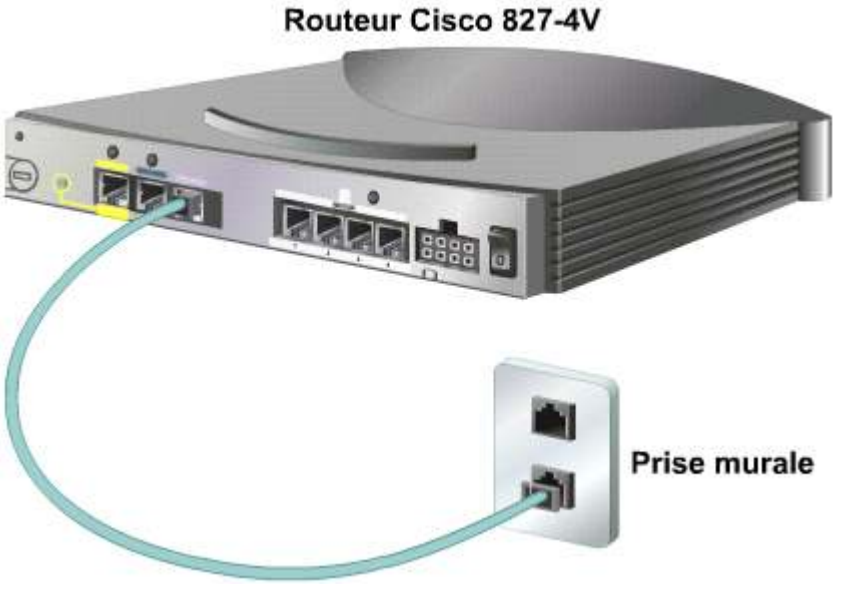
La page suivante traite de la connexion DSL pour un routeur.

5.2 Câblage des réseaux WAN

5.2.5 Routeurs et connexions DSL

Cette page présente les routeurs et les connexions DSL.

Le routeur ADSL Cisco 827 est équipé d'une interface ADSL (*Asymmetric Digital Subscriber Line*). 1



Pour raccorder une ligne ADSL au port ADSL d'un routeur, procédez comme suit:

- Reliez le cordon du téléphone au port ADSL du routeur.
- Reliez l'autre extrémité du cordon à la prise téléphonique.

Pour raccorder un routeur en vue d'un service DSL, utilisez un cordon de téléphone équipé de connecteurs RJ-11. La technologie DSL fonctionne via les lignes téléphoniques standard, à l'aide des broches 3 et 4 d'un connecteur RJ-11 standard.

La page suivante traite des connexions par câble.

5.2 Câblage des réseaux WAN

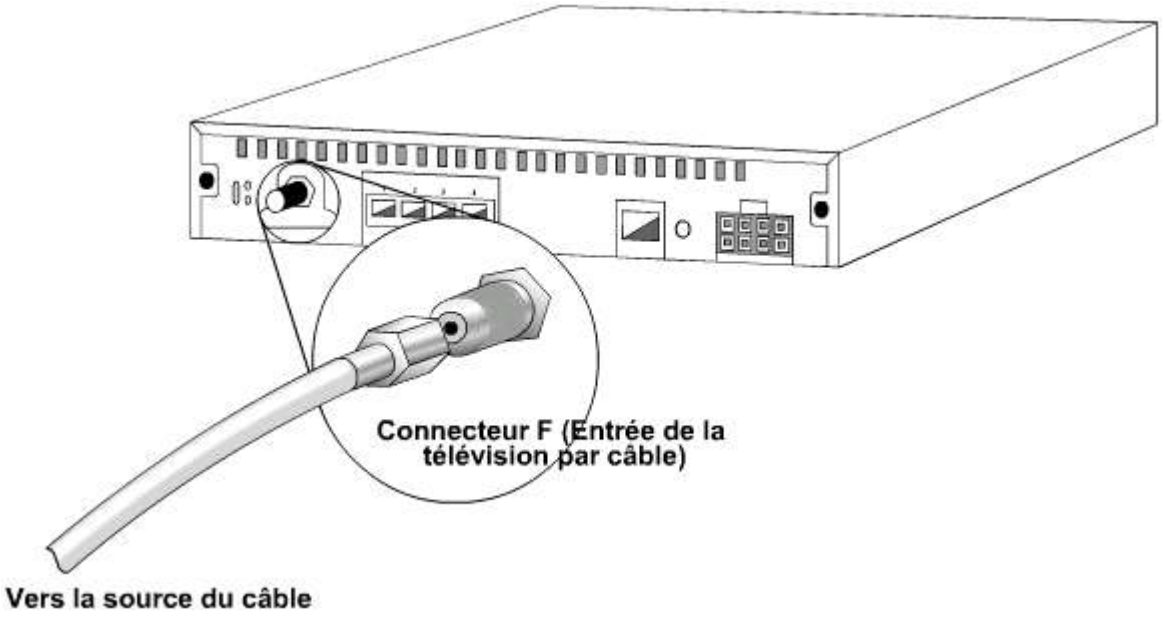
5.2.6 Routeurs et connexions par câble

Cette page traite de la connexion des routeurs aux systèmes par câble.

Le routeur d'accès au câble Cisco uBR905 offre un accès réseau haut débit via la télédiffusion par câble aux abonnés résidentiels et de petits bureaux/bureaux à domicile (SOHO). Le modèle uBR905 comporte une interface câble coaxial, ou connecteur F, qui se raccorde directement au système de câblage. Le routeur et le système de câblage sont reliés par le biais d'un câble coaxial et d'un connecteur BNC.

Pour relier le routeur d'accès au câble Cisco uBR905 au système de câblage, procédez comme suit:

- Vérifiez que le routeur n'est pas branché à une prise de courant.
- Localisez le câble coaxial RF qui sort de la prise murale de télévision par câble.
- Le cas échéant, installez un répartiteur de câble/coupleur directionnel pour séparer les signaux de la télévision et de l'ordinateur. Si nécessaire, installez également un filtre passe-haut pour éviter toute interférence entre les signaux de la télévision et de l'ordinateur.
- Raccordez le câble coaxial au connecteur F du routeur. 1



Maintenez fermement le connecteur en veillant à bien l'insérer, puis faites-lui opérer une rotation d'un sixième de tour à l'aide d'une clé.

- Veillez à ce que tous les connecteurs du câble coaxial, les répartiteurs intermédiaires, les coupleurs ou les blocs de mise à la terre soient solidement fixés de la prise au routeur Cisco uBR905.

ATTENTION: Ne serrez pas le connecteur de façon excessive, sous peine de l'endommager. N'utilisez pas de clé dynamométrique car vous risqueriez de trop faire tourner le connecteur. Il est recommandé de lui faire faire un sixième de tour après son insertion.

La page suivante traite des connexions console.

5.2 Câblage des réseaux WAN

5.2.7 Configuration des connexions console

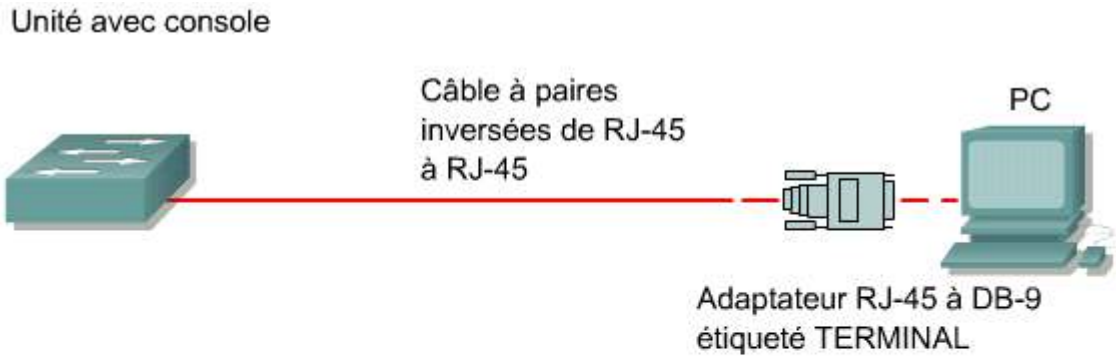
Cette page décrit la configuration des connexions console.

Pour la configuration initiale de l'équipement Cisco, une connexion d'administration doit être directement liée à l'équipement. Pour l'équipement Cisco, cette liaison d'administration est appelée «port console». Le port console permet de surveiller et de configurer un concentrateur, un commutateur ou un routeur Cisco.

Un câble à paires inversées équipé de connecteurs RJ-45 relie le terminal et le port console. Le câble à paires inversées, ou câble console, présente une configuration différente de celle des câbles RJ-45 droits ou croisés que l'on utilise dans le cas d'Ethernet ou de RNIS BRI. Un câble à paires inversées présente la configuration de broches suivante:

De 1 à 8
De 2 à 7
De 3 à 6
De 4 à 5
De 5 à 4
De 6 à 3

La configuration d'une connexion entre le terminal et le port console Cisco s'effectue en deux étapes. Raccordez tout d'abord les équipements à l'aide d'un câble à paires inversées (du port console du routeur au port série de la station de travail). Vous devrez peut-être installer un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25 pour le PC ou le terminal. 1



- Les PC nécessitent un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25.
- Les paramètres du port COM sont 9 600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.
- Un accès hors bande à la console est fourni.
- Le port AUX du commutateur peut être utilisé pour une console connectée par modem.

Puis, configurez l'application d'émulation du terminal à l'aide des paramètres de port COM suivants: 9600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.

Le port AUX fournit une gestion hors bande via un modem. Pour pouvoir l'utiliser, vous devez le configurer par le biais du port console. Le port AUX utilise également les paramètres 9 600 bits/s, 8 bits de données, sans parité, 1 bit d'arrêt et sans contrôle de flux.

Lors de l'activité de TP, les étudiants vont établir une connexion console à un routeur ou à un commutateur.

L'activité de média interactive propose une vue détaillée d'un câble console.

Cette page conclut la leçon. La page suivante résume les principaux points du module.

Activité de TP

Exercice: Établissement d'une connexion console avec un routeur ou un commutateur

L'objectif de ce TP est de créer une connexion console d'un PC à un routeur et à un commutateur à l'aide du câble approprié.

Activité de média interactive

Agrandissement: Câble console

Dans cette vue agrandie, l'étudiant peut observer un câble console.

Résumé

Cette page résume les sujets traités dans ce module.

Ethernet, la technologie LAN la plus répandue, peut être mis en œuvre sur tout un éventail de médias. Les technologies Ethernet offrent des débits variés, de 10 Mbits/s à Gigabit Ethernet, pouvant être appliqués à différents domaines d'un réseau. Les besoins en matière de médias et de connecteurs diffèrent selon les implémentations Ethernet.

Le connecteur d'une carte réseau doit correspondre au média. Un connecteur BNC (*Bayonet Nut Connector*) est nécessaire pour le raccordement au câble coaxial. Un connecteur pour fibre optique permet le raccordement au média à fibre optique. Le connecteur RJ-45 utilisé avec un fil à paires torsadées est le type de connecteur le plus couramment utilisé dans les implémentations LAN Ethernet.

Lorsque vous utilisez un fil à paires torsadées pour relier les équipements, vous devez également déterminer l'ordre des fils (configuration des broches). Un câble croisé permet de relier deux équipements similaires, tels que deux PC. Un câble droit sert à relier deux équipements différents, ce qui est le cas des connexions entre un commutateur et un PC. Un câble à paires inversées permet de connecter un PC au port console d'un routeur.

Les répéteurs régénèrent et resynchronisent les signaux réseau pour leur permettre de voyager sur de plus longues distances via le média. Les concentrateurs sont des répéteurs multiports. Les données qui arrivent sur le port d'un concentrateur se répètent par impulsion électrique sur tous les autres ports connectés au même segment du réseau, à l'exception de celui qui a reçu les données. Les concentrateurs, comme leur nom l'indique, constituent souvent un point de connexion central pour un réseau LAN Ethernet.

Un réseau sans fil implique un câblage beaucoup moins important que les autres types de réseau. Seuls les points d'accès du réseau peuvent faire l'objet d'un câblage permanent. La communication sans fil s'appuie sur des équipements appelés «émetteurs» et «récepteurs». L'émetteur convertit les données source en ondes électromagnétiques (EM), qu'il envoie au récepteur. Puis, le récepteur reconvertit ces ondes électromagnétiques en données pour les envoyer à la destination. Les technologies sans fil IR (infrarouge) et RF (radiofréquence) sont les plus répandues dans le domaine des réseaux.

Dans certains cas, il peut s'avérer nécessaire de diviser un LAN de taille importante en plusieurs petits segments, plus faciles à gérer. Vous pouvez utiliser des équipements de type ponts, commutateurs, routeurs et passerelles pour définir les segments du réseau et les relier les uns aux autres.

Un pont utilise l'adresse MAC de destination pour déterminer s'il doit filtrer la trame, la diffuser ou la copier sur un autre segment. Placé de façon stratégique, un pont améliore considérablement les performances réseau.

Les commutateurs sont parfois qualifiés de « ponts multiports ». Bien que ces deux équipements présentent des points communs, un commutateur est plus sophistiqué qu'un pont. Les commutateurs fonctionnent à des débits beaucoup plus élevés que les ponts et peuvent accepter de nouvelles fonctionnalités, telles que les LAN virtuels (VLAN).

Les routeurs sont responsables du routage des paquets de données de la source à la destination au niveau du LAN, ainsi que de la connectivité au WAN. Dans l'environnement d'un LAN, le routeur contrôle les broadcasts, fournit les services de résolution d'adresse du type ARP et RARP et peut segmenter le réseau via une structure de sous-réseaux.

En règle générale, les ordinateurs communiquent les uns avec les autres à l'aide de protocoles de requête/réponse. L'un envoie une requête de service, et l'autre reçoit cette requête et y répond. Les ordinateurs membres d'un réseau d'égal à égal se comportent comme des partenaires égaux (ou «pairs»). En tant que pair, chaque ordinateur peut tour à tour assurer la fonction de client et de serveur. Dans un environnement client-serveur, les services réseau tournent sur un ordinateur dédié appelé « serveur ». Le serveur répond aux requêtes des clients.

Les liaisons série haut débit, RNIS, DSL et modem câble sont des types de connexion WAN. Chacun d'entre eux nécessite un média et un connecteur spécifiques. Pour relier le port RNIS BRI à l'équipement de l'opérateur télécom, il convient d'utiliser un câble droit à paire torsadée non blindée (UTP) de catégorie 5 avec des connecteurs RJ-45. On utilise un cordon de téléphone et un connecteur RJ-11 pour raccorder un routeur dans le cas du service DSL. Un câble coaxial et un connecteur BNC permettent de connecter un routeur en vue d'un accès par le câble.

Outre le type de connexion, il convient de déterminer les connecteurs à utiliser (ETTD ou ETCD) au niveau des équipements d'interconnexion. L'ETTD est le point d'extrémité du réseau privé d'un utilisateur au niveau de la liaison WAN. L'ETCD est, en général, le point auquel la responsabilité de la diffusion des données est reportée sur le fournisseur de services. Lorsque vous vous connectez directement à un fournisseur de services ou à un équipement tel qu'une unité CSU/DSU qui doit exécuter le signal de synchronisation, le routeur constitue un équipement ETTD et doit être équipé d'un câble série du même type. Tel est généralement le cas des routeurs. Cependant, le routeur doit, dans certains cas, être l'équipement ETCD.

Câblage des réseaux LAN et WAN

- Les répéteurs, les concentrateurs, les ponts et les commutateurs sont des équipements LAN courants.
- Il existe deux types principaux de réseau LAN, d'égal à égal et client-serveur.
- Les réseaux WAN font appel à la transmission série. Les types de connexion WAN comprennent RNIS, DSL et le modem câble.

6-Notions de base sur ethernet

Vue d'ensemble

Ethernet est aujourd'hui la technologie de réseau local dominante sur le plan mondial. Ethernet est une famille de technologies de réseau local que le modèle de référence OSI rend plus facile à appréhender. Tous les réseaux locaux doivent traiter le problème de base qui est l'attribution de noms à chaque station ou nœud. Les spécifications Ethernet prennent en charge différents médias, bandes passantes et autres variantes des couches 1 et 2. Cependant, le format de trame de base et le système d'adressage sont les mêmes pour toutes les variantes d'Ethernet.

Différentes stratégies MAC ont été élaborées pour permettre à plusieurs stations d'accéder aux médias physiques et aux équipements de réseau. Il est important d'expliquer comment les équipements de réseau obtiennent l'accès aux médias de réseau pour que les étudiants puissent comprendre et dépanner le réseau tout entier.

Ce module porte sur certains des objectifs des examens CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
			• Description des communications réseau à l'aide des modèles en couche • Évaluation des règles de gestion des paquets

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
			• Évaluation des règles de gestion des paquets

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Description des propriétés physiques, électriques et mécaniques ainsi que des normes associées aux médias optique, sans fil et cuivre utilisés dans les réseaux • Description des topologies et des problèmes physiques liés au câblage des LAN les plus courants • Comparaison entre les domaines de collision et ceux de broadcast ; description du processus de segmentation de réseau • Explication des méthodes de détection et de gestion des collisions dans un système Ethernet • Explication des concepts fondamentaux associés à la technique d'accès au média Ethernet

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
6.1	Notions de base sur Ethernet
6.2	Fonctionnement d'Ethernet

- Décrire les notions de base de la technologie Ethernet
- Expliquer les règles d'attribution de nom de la technologie Ethernet
- Expliquer la relation entre Ethernet et le modèle OSI
- Décrire le processus de verrouillage de trame et la structure de trame Ethernet
- Lister les noms des champs des trames Ethernet et leur objet
- Identifier les caractéristiques de CSMA/CD
- Décrire la synchronisation, l'espacement intertrame et la réémission temporisée après une collision
- Définir les erreurs et les collisions Ethernet

- Expliquer le concept d'autonégociation en fonction de la vitesse et du mode duplex configuré

6.1 Notions de base sur Ethernet

6.1.1 Introduction à Ethernet

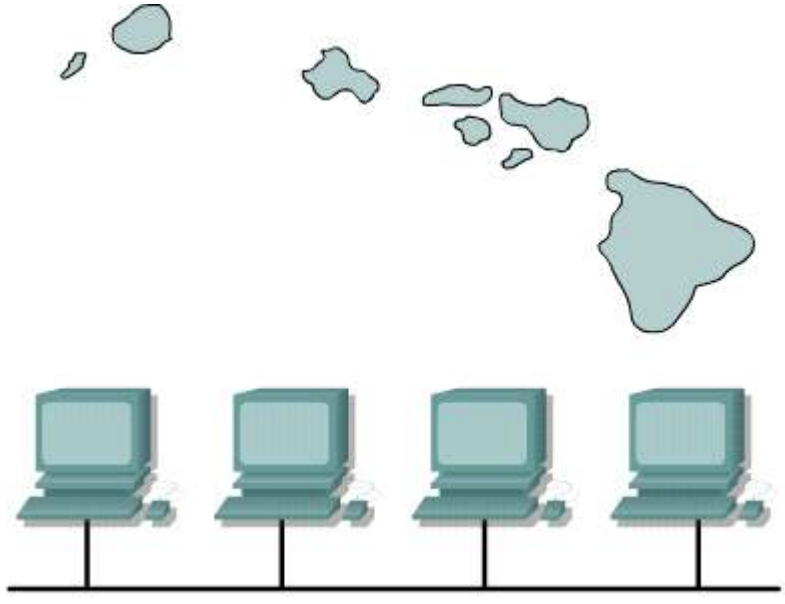
Cette page présente une introduction à Ethernet. La plus grande partie du trafic sur Internet débute et aboutit sur des connexions Ethernet. Depuis ses débuts dans les années 70, Ethernet a évolué pour répondre à la demande accrue en réseaux locaux haut débit. Lorsque les médias à fibre optique ont été introduits, Ethernet s'est adapté pour tirer parti de la bande passante supérieure et du faible taux d'erreur qu'offre cette technologie. À présent, le même protocole qui transportait les données à 3 Mbits/s en 1973 assure des transmissions à 10 Gbits/s.

Le succès d'Ethernet est dû aux facteurs suivants:

- Simplicité et facilité de maintenance
- Capacité à incorporer de nouvelles technologies
- Fiabilité
- Faible coût d'installation et de mise à niveau

L'introduction de Gigabit Ethernet a étendu la technologie de réseau local originale à un tel point qu'Ethernet est maintenant une norme des réseaux MAN et WAN.

À l'origine, l'idée était de permettre à deux hôtes au moins d'utiliser le même média sans aucune interférence entre les signaux. Ce problème d'accès multiple de l'utilisateur à un média partagé a été étudié au début des années 70 à l'Université d'Hawaï. Un système nommé Alohanet a été développé pour donner à plusieurs stations des Iles Hawaï un accès structuré à la fréquence radio partagée dans l'atmosphère. 1



Ce travail a par la suite constitué la base de la méthode d'accès Ethernet connue sous l'acronyme CSMA/CD.

Le premier réseau local au monde a été la version originale d'Ethernet. Robert Metcalfe et ses collaborateurs de Xerox l'on conçu il y a plus de trente ans. La première norme Ethernet a été publiée en 1980 par un consortium de Digital Equipment Company, Intel et Xerox (DIX). Metcalfe souhaitant qu'Ethernet soit une norme standard dont tout le monde puisse bénéficier, elle a été publiée en tant que norme ouverte. Les premiers produits développés respectant la norme Ethernet ont été commercialisés au début des années 80. Ethernet transmettait alors à 10 Mbits/s sur un câble coaxial épais et sur une distance pouvant atteindre 2 kilomètres (km). Ce type de câble coaxial de la largeur d'un petit doigt était appelé thicknet.

En 1985, le comité de normalisation IEEE pour les réseaux locaux et métropolitains a publié des normes pour les réseaux locaux. Ces normes commencent par le numéro 802. La norme Ethernet porte le numéro 802.3. L'IEEE a voulu faire en sorte que ses normes soient compatibles avec l'ISO (International Standards

Organization) et le modèle OSI. Pour ce faire, la norme IEEE 802.3 devait répondre aux besoins de la couche 1 et de la partie inférieure de la couche 2 du modèle OSI. En conséquence, certaines modifications mineures de la norme Ethernet originale ont été apportées à la 802.3.

Les différences entre les deux normes sont si mineures que n'importe quelle carte réseau Ethernet peut transmettre et recevoir à la fois des trames Ethernet et 802.3. Pour l'essentiel, les normes Ethernet et IEEE 802.3 sont identiques.

La bande passante de 10 Mbits/s d'Ethernet était plus que suffisante pour les lents PC des années 80. Au début des années 90, ceux-ci devinrent bien plus rapides, les tailles des fichiers augmentèrent et des goulets d'étranglement commencèrent de se produire. La plupart des problèmes étaient causés par la faible disponibilité de la bande passante. En 1995, l'IEEE annonça une norme pour un Ethernet à 100 Mbits/s. Vinrent ensuite des normes pour Gigabit Ethernet en 1998 et 1999.

Toutes les normes sont, pour l'essentiel, compatibles avec la norme Ethernet originale. Ainsi, une trame Ethernet pourrait quitter la carte réseau d'un PC en empruntant un câble coaxial ancien à 10 Mbits/s, être dirigée sur une liaison à fibre optique Ethernet à 10 Gbits/s et aboutir sur une carte réseau à 100 Mbits/s. Tant que la trame reste sur les réseaux Ethernet, elle n'est pas modifiée. Pour cette raison, Ethernet est réputé très évolutif. La bande passante du réseau pourrait être augmentée plusieurs fois sans entraîner de modification de la technologie Ethernet.

La norme Ethernet originale a été modifiée plusieurs fois pour gérer de nouveaux médias et des taux de transmission plus élevés. Ces modifications fournissent des normes pour les nouvelles technologies et maintiennent la compatibilité entre les variantes d'Ethernet.

La page suivante explique les règles d'attribution de noms pour la famille de réseaux Ethernet.

6.1 Notions de base sur Ethernet

6.1.2 Règles d'attribution de noms Ethernet par l'IEEE

Cette page met l'accent sur les règles d'attribution de noms Ethernet développées par l'IEEE.

Ethernet n'est pas une technologie de réseau unique mais une famille de technologies qui inclut l'existant, Fast Ethernet et Gigabit Ethernet. Les vitesses d'Ethernet s'échelonnent entre 10, 100, 1000 ou 10 000 Mbits/s. Le format de trame de base et les sous-couches IEEE des couches OSI 1 et 2 restent cohérents quelle que soit la forme d'Ethernet.

Chaque fois qu'Ethernet doit être étendu pour ajouter un nouveau média ou une nouvelle capacité, l'IEEE publie un nouveau supplément à la norme 802.3. Les nouveaux suppléments sont identifiés par une ou deux lettres (p. ex. 802.3u). Une description abrégée, appelée identificateur, est également affectée au supplément. 1

Vitesse	Méthode de signalisation	Média
10	BASE	2
100	LARGE	5
1000		-T
10G		-TX
		-SX
		-LX

La description abrégée comporte les éléments suivants:

- Un chiffre qui indique le nombre de Mbits/s transmis
- Des lettres pour indiquer que la signalisation de la bande de base est utilisée
- Une ou plusieurs lettres de l'alphabet indiquant le type de média utilisé. Par exemple, F = câble à fibre optique et T = paire de cuivre torsadée non blindée

Ethernet repose sur la signalisation de bande de base, qui utilise la totalité de la bande passante du média de transmission. Le signal de données est transmis directement sur le média de transmission.

Dans la signalisation à large bande, le signal de données n'est plus placé directement sur le média de transmission. Ethernet utilisait la signalisation à large bande dans le cadre de la norme 10Broad36. 10Broad36 est la norme de l'IEEE correspondant à un réseau Ethernet 802.3 qui utilise la transmission à large bande avec un câble coaxial épais fonctionnant à 10 Mbits/s. 10Broad36 est à présent considérée comme obsolète. Un signal analogique ou de porteuse est modulé par le signal de données puis transmis. Les émissions radiophoniques et la TV par câble utilisent la signalisation à large bande.

L'IEEE ne peut pas forcer les fabricants à se conformer complètement à une quelconque norme. L'IEEE a pour cela deux objectifs principaux:

- Fournir les informations nécessaires pour construire des équipements qui sont conformes aux normes Ethernet
- Promouvoir l'innovation auprès des fabricants

Les étudiants vont effectuer l'activité de média interactive afin de mieux identifier les normes IEEE 802.

La page suivante explique Ethernet et le modèle OSI.

Activité de média interactive

Glisser-Positionner: Normes IEEE 802

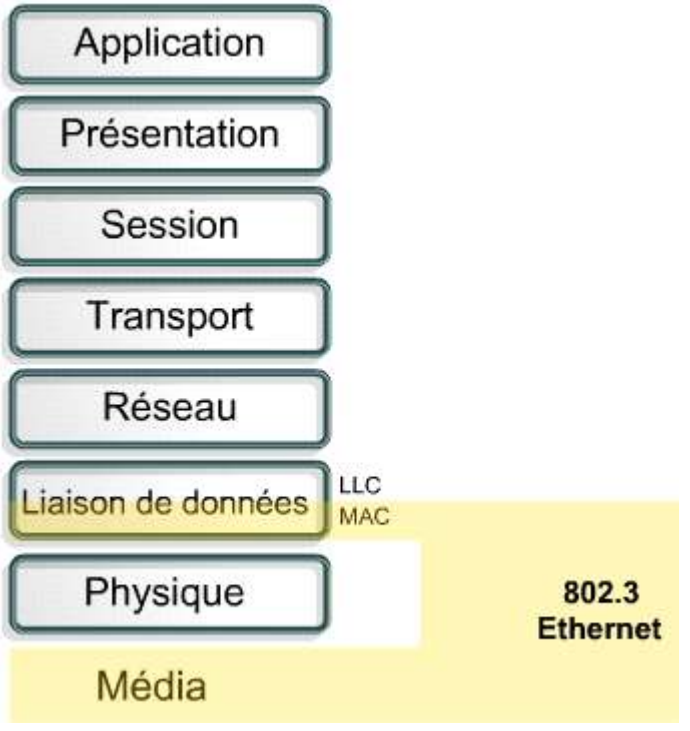
Cette activité teste la connaissance des normes IEEE 802.

6.1 Notions de base sur Ethernet

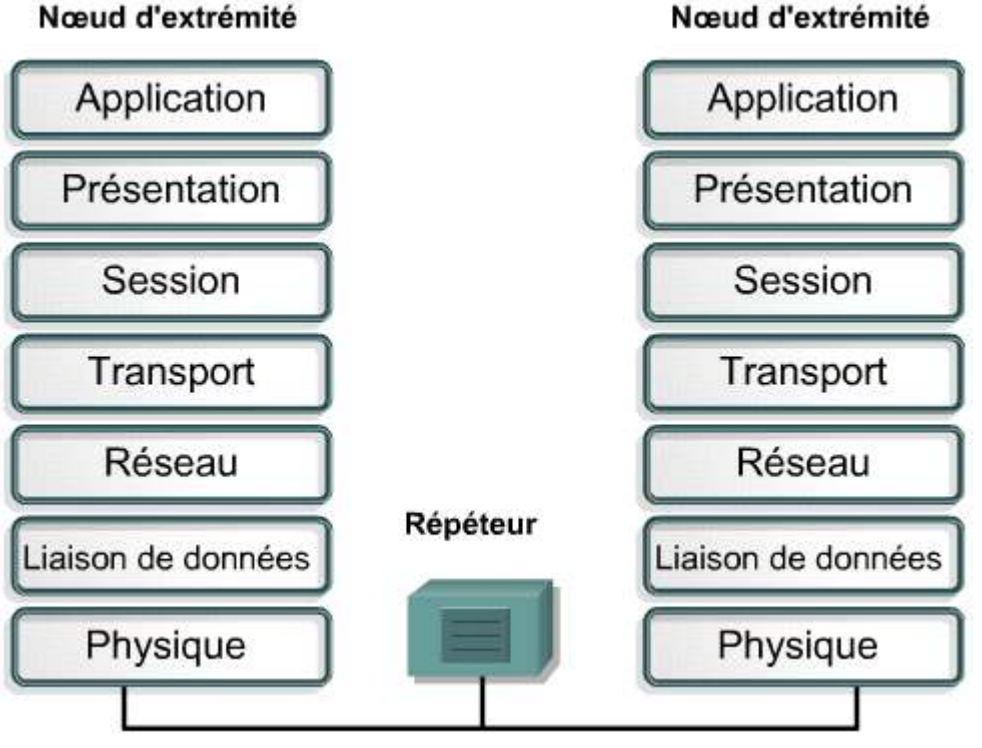
6.1.3 Ethernet et le modèle OSI

Cette page explique la relation entre Ethernet et le modèle OSI.

Ethernet opère dans deux domaines du modèle OSI. Il s'agit de la moitié inférieure de la couche liaison de données, que l'on appelle sous-couche MAC, et la couche physique. 1



Les données qui transitent entre deux stations Ethernet passent souvent par un répéteur. Toutes les stations du même domaine de collision voient le trafic passant par un répéteur. 2

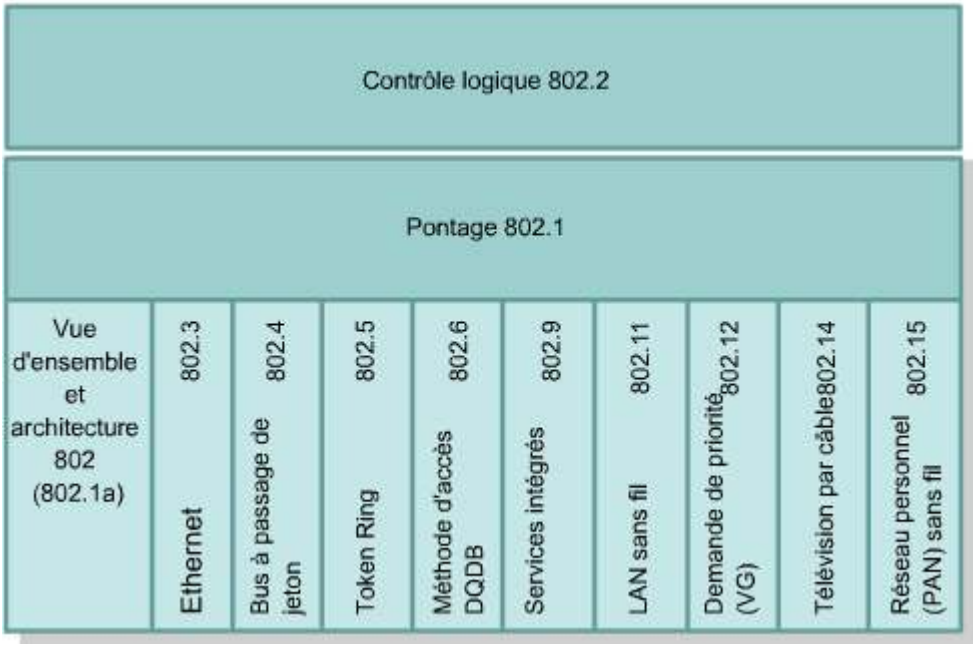


Un domaine de collision est un domaine partagé. Les problèmes qui proviennent d'une partie d'un domaine de collision auront en principe un impact sur le domaine de collision tout entier.

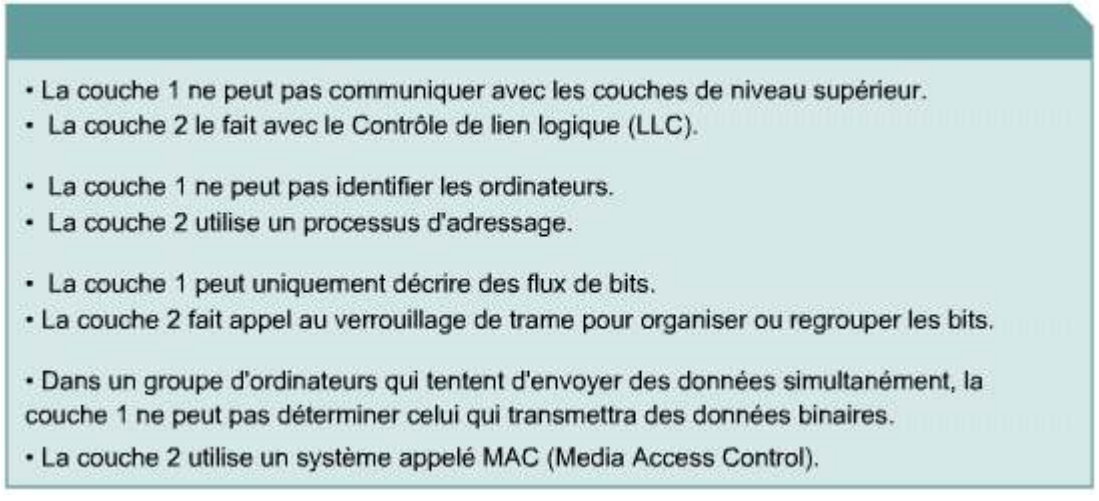
Un répéteur transmet le trafic à tous les autres ports. Il n'envoie jamais de trafic par le port qui a servi à le recevoir. Tout signal détecté par le répéteur sera transmis. Si le signal subit une dégradation due à l'atténuation ou au bruit, le répéteur tentera de reconstruire et de régénérer le signal.

Afin de garantir une bande passante et une opérabilité minimales, les normes spécifient le nombre maximum de stations par segment, la longueur maximum de segment, ainsi que le nombre maximum de répéteurs entre stations. Les stations séparées par des répéteurs se trouvent à l'intérieur du même domaine de collision. Les stations séparées par des ponts ou des routeurs se trouvent dans des domaines de collision différents.

La figure 3

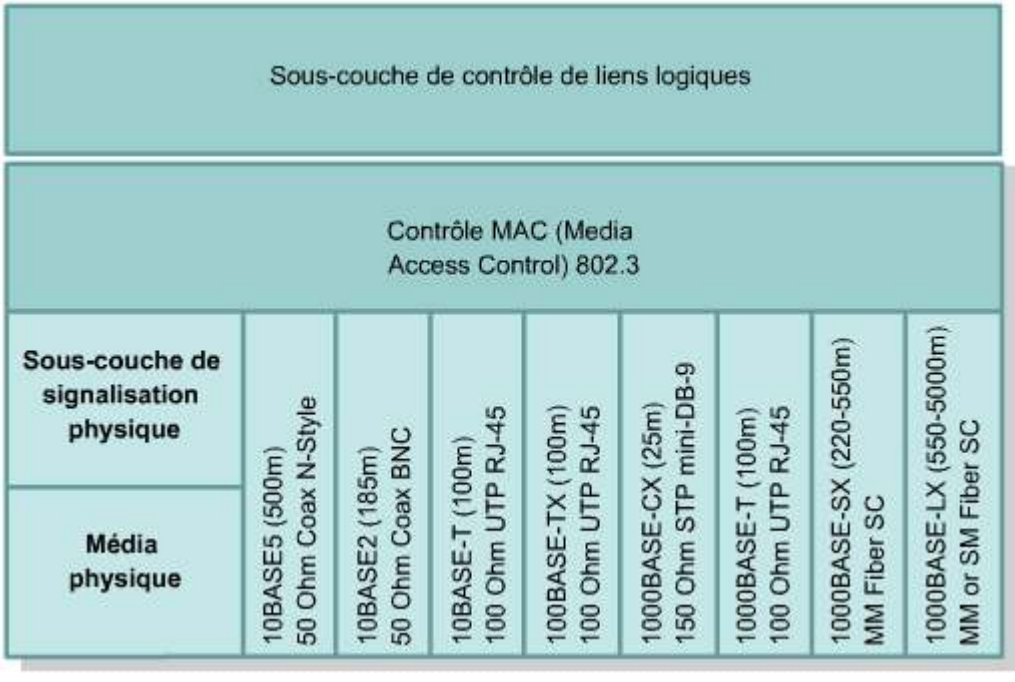

Contrôle logique 802.2
Pontage 802.1
Vue d'ensemble et architecture 802 (802.1a)
802.3 Ethernet
802.4 Bus à passage de jeton
802.5 Token Ring
802.6 Méthode d'accès DQDB
802.9 Services intégrés
802.11 LAN sans fil
802.12 Demande de priorité (VG)
802.14 Télévision par câble
802.15 Réseau personnel (PAN) sans fil

fait correspondre diverses technologies Ethernet avec la partie inférieure de la couche 2 OSI et avec l'ensemble de la couche 1. Sur la couche 1, Ethernet gère des signaux, des flots de bits qui circulent sur le média, des composants qui placent les signaux sur le média et diverses topologies. La couche 1 Ethernet joue un rôle clé dans le cadre des communications entre les équipements. Toutefois, utilisées seules, ces fonctions ne sont pas suffisantes. La couche 2 traite ces restrictions. 4


• La couche 1 ne peut pas communiquer avec les couches de niveau supérieur.
• La couche 2 le fait avec le Contrôle de lien logique (LLC).
• La couche 1 ne peut pas identifier les ordinateurs.
• La couche 2 utilise un processus d'adressage.
• La couche 1 peut uniquement décrire des flux de bits.
• La couche 2 fait appel au verrouillage de trame pour organiser ou regrouper les bits.
• Dans un groupe d'ordinateurs qui tentent d'envoyer des données simultanément, la couche 1 ne peut pas déterminer celui qui transmettra des données binaires.
• La couche 2 utilise un système appelé MAC (Media Access Control).

Les sous-couches liaison de données contribuent de façon significative à la compatibilité technologique et aux communications informatiques. La sous-couche MAC est responsable des composants physiques qui seront utilisés pour communiquer les informations. La sous-couche LLC (*Logical Link Control – contrôle de lien logique*) reste relativement indépendante de l'équipement physique qui sera utilisé pour le processus de communication.

La figure 5


Sous-couche de contrôle de liens logiques
Contrôle MAC (Media Access Control) 802.3
Sous-couche de signalisation physique
Média physique
10BASE5 (500m) 50 Ohm Coax N-Style
10BASE2 (185m) 50 Ohm Coax BNC
10BASE-T (100m) 100 Ohm UTP RJ-45
100BASE-TX (100m) 100 Ohm UTP RJ-45
1000BASE-CX (25m) 150 Ohm STP mini-DB-9
1000BASE-T (100m) 100 Ohm UTP RJ-45
1000BASE-SX (220-550m) MM Fiber SC
1000BASE-LX (550-5000m) MM or SM Fiber SC

fait correspondre diverses technologies Ethernet avec la partie inférieure de la couche 2 OSI et avec l'ensemble de la couche 1. Alors qu'il existe d'autres variétés d'Ethernet, celles illustrées sont les plus largement utilisées.

L'activité de média interactive passe en revue les couches du modèle OSI.

La page suivante explique le système d'adressage qu'utilisent les réseaux Ethernet.

Activité de média interactive

Glisser-Positionner: Modèle OSI

À la fin de cette activité, l'étudiant doit être en mesure d'identifier les 7 couches du modèle OSI, y compris les deux sous-couches liaison de données.

6.1 Notions de base sur Ethernet

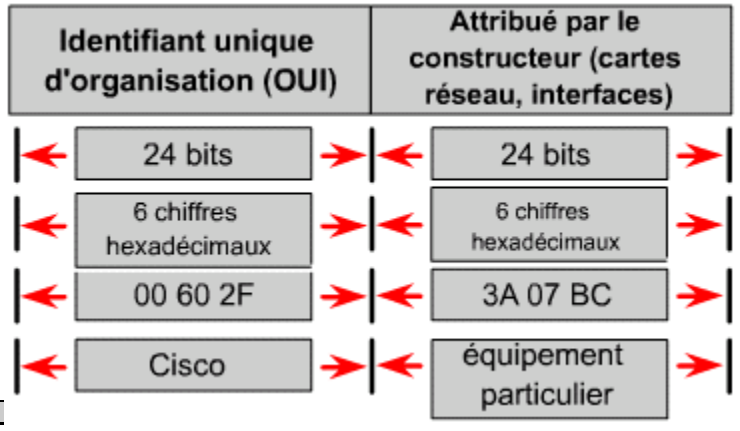
6.1.4 Attribution de noms

Cette page décrit les adresses MAC qu'utilisent les réseaux Ethernet.

Un système d'adressage est nécessaire pour identifier de façon unique les ordinateurs et les interfaces qui permettent une distribution locale des trames sur Ethernet. 1



Ethernet utilise des adresses MAC qui comportent 48 bits et qui sont exprimées à l'aide de douze chiffres hexadécimaux. Les six premiers chiffres hexadécimaux, qui sont administrés par l'IEEE, identifient le fabricant ou le fournisseur. Cette partie de l'adresse MAC est appelée identifiant unique d'organisation (OUI). Les six autres chiffres hexadécimaux forment le numéro de série d'interface ou une autre valeur administrée par le fabricant. 2



On dit parfois des adresses MAC qu'elles sont rémanentes (BIA - *burned-in adresses*) parce qu'elles demeurent en mémoire morte (ROM) et sont copiées en mémoire vive (RAM) lors de l'initialisation de la carte réseau.

Au niveau de la couche liaison de données, des en-têtes et des en-queues MAC sont ajoutés aux données de la couche supérieure. Ces en-têtes et en-queues contiennent des informations de contrôle destinées à la couche liaison de données du système de destination. Les données des couches supérieures sont encapsulées dans la trame liaison de données, entre l'en-tête et l'en-queue, puis envoyées sur le réseau.

La carte réseau utilise l'adresse MAC afin de déterminer si un message doit être transmis aux couches supérieures du modèle OSI. Elle n'utilise pas de temps processeur pour effectuer cette évaluation, ce qui améliore les temps de communication sur le réseau Ethernet.

Sur un réseau Ethernet, lorsqu'un équipement envoie des données, il peut ouvrir une voie de communication en utilisant l'adresse MAC de l'autre équipement. L'équipement source attache un en-tête avec l'adresse MAC de l'équipement de destination prévu, et envoie des données sur le réseau. Tandis que les données se déplacent sur le média réseau, la carte réseau de chaque équipement du réseau vérifie si son adresse MAC correspond à l'adresse physique de destination transportée par la trame de données. En l'absence de correspondance, la carte réseau ignore la trame de données. Lorsque les données atteignent le nœud de destination, la carte réseau fait une copie et transmet la trame aux couches OSI. Sur un réseau Ethernet, tous les nœuds doivent examiner l'en-tête MAC.

Tous les équipements qui sont connectés à un réseau local Ethernet possèdent des interfaces adressées MAC. Cela inclut les stations de travail, imprimantes, routeurs et commutateurs.

La page suivante porte sur les trames de la couche 2.

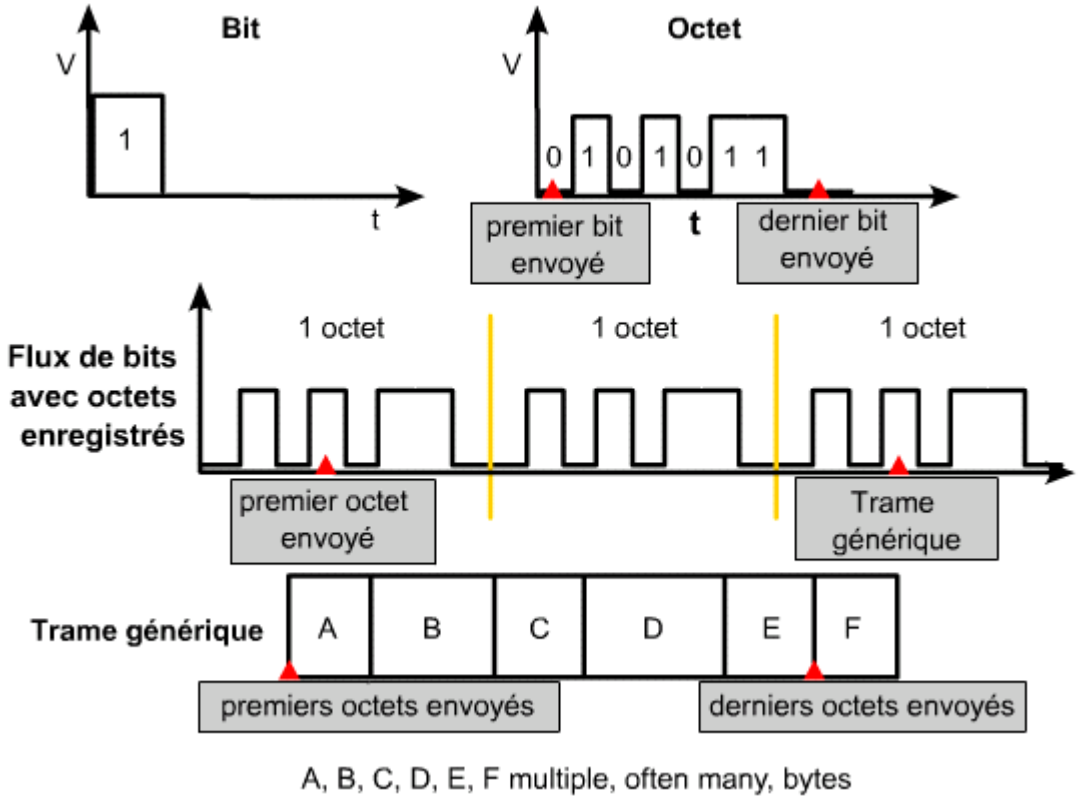
Cette page explique comment les trames sont créées sur la couche 2 du modèle OSI.

Les trains binaires codés sur un média physique constituent une réalisation technologique remarquable. Cependant, à eux seuls, ils ne suffisent pas à assurer la communication. Le verrouillage de trame permet de récupérer des informations essentielles qu'il n'était pas possible d'obtenir uniquement avec les trains binaires codés. Ces informations sont les suivantes:

- Quels sont les ordinateurs en communication?
- Quand commence la communication entre des ordinateurs et quand se termine-t-elle?
- Quelles erreurs se sont produites lors de la communication entre les ordinateurs?
- Quel sera le prochain ordinateur à communiquer?

Le verrouillage de trame est le processus d'encapsulation de la couche 2. Une trame est une unité de données de protocole de couche 2.

Un graphique de tension en fonction du temps pourrait être utilisé pour visualiser les bits. Cependant, il peut s'avérer trop difficile de représenter sous forme de graphique les informations d'adresse et de contrôle pour les unités de données plus importantes. Vous pouvez également utiliser le schéma de structure de trame, qui est articulé sur le diagramme de tension en fonction du temps. Les schémas de format de trame se lisent de gauche à droite, comme un oscillogramme. Les schémas de structure de trame font apparaître différents regroupements de bits (ou champs), qui remplissent d'autres fonctions. [1]



Il existe plusieurs types de trame différents, décrits par diverses normes. Une trame générique comprend des sections appelées champs. Chaque champ est constitué d'octets. [2]

Noms des champs				
A	B	C	D	E
Champ Début de trame	Champ Adresse	Champ Type/Longueur	Champ Données	Champ FCS

Les noms des champs sont les suivants:

- Champ de début de trame
- Champ d'adresse
- Champ de longueur/de type
- Champ de données
- Champ FCS (*Frame Check Sequence* = Séquence de contrôle de trame)

Les ordinateurs connectés à un média physique doivent pouvoir signaler qu'ils s'apprêtent à transmettre une trame. Différentes technologies apportent une solution. Quelle que soit la technologie, toutes les trames débutent par une séquence d'octets pour signaler la transmission des données.

Toutes les trames contiennent des informations d'identification, telles que le nom du nœud source, ou adresse MAC source, et celui du nœud de destination, ou adresse MAC de destination.

La plupart des trames contiennent des champs spécialisés. Dans certaines technologies, un champ de longueur indique la longueur exacte de la trame en octets. Certaines trames comportent un champ de type précisant le protocole de couche 3 utilisé par l'équipement qui veut envoyer des données.

Les trames sont utilisées pour envoyer des données de couche supérieure, puis des données d'application utilisateur d'une source à une destination. Le paquet de données inclut le message à envoyer ou les données d'application utilisateur. À des fins de synchronisation, d'autres octets peuvent être ajoutés pour que les trames aient une longueur minimale. Des octets LLC sont également ajoutés au champ de données dans les trames IEEE standard. La sous-couche LLC prend les données de protocole réseau, c'est-à-dire un paquet IP, et y ajoute des informations de contrôle pour faciliter l'acheminement de ce paquet IP jusqu'au nœud de destination. La couche 2 communique avec les couches de niveau supérieur par le biais de la sous-couche LLC.

Toutes les trames, ainsi que les bits, les octets et les champs qu'elles contiennent, peuvent comporter des erreurs provenant d'une multitude de sources. Le champ de la séquence de contrôle de trame (FCS) contient un numéro, calculé par l'ordinateur source, qui repose sur les données contenues dans la trame. Ce numéro est ajouté à la fin de la trame qui est envoyée. Lorsque le nœud de destination reçoit la trame, il calcule à nouveau la séquence de contrôle de trame et la compare à celle qui est incluse dans la trame. Si les deux numéros sont différents, il y a une erreur et la trame est abandonnée.

Étant donné que la source ne peut pas détecter que la trame a été abandonnée, la retransmission doit être lancée par des protocoles orientés connexion de couche supérieure fournissant le contrôle de flux de données. Habituellement la retransmission a lieu, parce que ces protocoles, tels que TCP, s'attendent à ce qu'un accusé de réception de trame (ACK) soit envoyé par la station homologue dans un laps de temps donné.

Il y a trois façons de calculer le numéro de séquence de contrôle de trame:

- **Code de redondance cyclique (CRC)** – exécution des calculs sur les données.
- **Parité bidimensionnelle** – place des octets individuels dans une matrice bidirectionnelle et effectue des contrôles de redondance verticalement et horizontalement sur la matrice, ce qui crée ainsi un octet supplémentaire produisant un nombre pair ou impair de 1 binaires.
- **Somme de contrôle Internet** – somme résultant de l'addition des valeurs de tous les bits de données.

Le nœud qui transmet les données doit obtenir l'attention des autres équipements pour commencer et terminer une trame. Le champ de longueur indique où la trame se termine. La trame se termine après la séquence de contrôle de trame. Il y a parfois une séquence formelle d'octets appelée «délimiteur de fin de trame».

La page suivante présente la structure de trame d'un réseau Ethernet.

6.1 Notions de base sur Ethernet

6.1.6 Structure de trame Ethernet

Cette page décrit la structure de trame des réseaux Ethernet.

Sur la couche liaison de donnée, la structure de trame est pratiquement identique pour toutes les vitesses d'Ethernet, de 10 Mbits/s à 10 000 Mbits/s. [1]



Calcul FCS						
Préambule	SFD	Destination	Source	Type de longueur	Données : Remplissage	FCS
7	1	6	6	2	de 46 à 1500	4

Champs des trames Ethernet IEEE 802.3

Octets	Description
• 7	Préambule
• 1	Délimiteur de début de trame (SFD)
• 6	Adresse MAC de destination
• 6	Adresse MAC source
• 2	Champ Longueur/Type (si la longueur est inférieure à 0600 en hexadécimal, sinon Type de protocole)
• de 46 à 1500	Données* (si inférieures à 46 octets, des données de remplissage doivent être ajoutées à la fin)
• 4	Séquence de contrôle de trame (Somme de contrôle CRC)

Cependant, au niveau de la couche physique, presque toutes les versions d'Ethernet sont différentes. À chaque vitesse est associé un ensemble distinct de règles de conception d'architecture.

Dans la version Ethernet qui a été développée par DIX avant l'adoption de la version IEEE 802.3, le préambule et le délimiteur de début de trame (SOF) ont été combinés en un champ unique. La configuration binaire était identique. Le champ de longueur/type comportait uniquement la longueur dans les premières versions d'IEEE et uniquement le type dans la version DIX. Ces deux utilisations du champ furent officiellement combinées dans la version IEEE ultérieure puisque les deux utilisations étaient courantes. [2]

Préambule	Destination	Source	Longueur	Données : Remplissage	FCS
8	6	6	2	de 46 à 1500	4

Octets	Description
• 8	Préambule (se termine par le modèle 10101011, le SFD 802.3)
• 6	Adresse MAC de destination
• 6	Adresse MAC source
• de 46 à 1500	Données* (si inférieures à 46 octets, des données de remplissage doivent être ajoutées à la fin)
• 2	Champ Type
• 4	Séquence de contrôle de trame (Somme de contrôle CRC)

Le champ de type Ethernet II est incorporé dans la définition de trame 802.3 actuelle. Lorsqu'un nœud reçoit une trame, il doit examiner le champ de longueur/type afin de déterminer quel protocole de couche supérieure est présent. Si la valeur de ces deux octets est égale ou supérieure à la valeur hexadécimale 0x0600 (1536 en notation décimale), alors le contenu du champ de données est décodé suivant le protocole indiqué. 3

- Norme introduite par DIX.
- Utilisé par les réseaux TCP/IP
- Utilise le champ Type pour déterminer un protocole de couche supérieure.
- Exemples de type :
  - 0x0806 = ARP
  - 0x0800 = IPv4

La structure de trame Ethernet II est celle utilisée dans les réseaux TCP/IP.

La page suivante décrit les informations incluses dans une trame.

6.1 Notions de base sur Ethernet

6.1.7 Champs des trames Ethernet

Cette page définit les champs utilisés dans une trame.

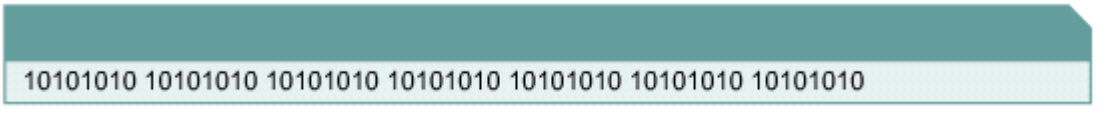
Une trame Ethernet 802.3 comprend les champs autorisés ou obligatoires suivants: 1

IEEE 802.3						
7	1	6	6	2	de 46 à 1500	4
Préambule	Délimiteur de début de trame	Adresse de destination	Adresse source	Type de longueur	En-tête et données 802.2	Séquence de contrôle de trame

Ethernet					
8	6	6	2	de 46 à 1500	4
Préambule	Adresse de destination	Adresse source	Type	Données	Séquence de contrôle de trame

- Préambule
- Délimiteur de début de trame (SOF)
- Adresse de destination
- Adresse source
- Longueur/Type
- En-tête et données
- Séquence de contrôle de trame (FCS)
- Extension

Le préambule est une succession de uns et de zéros permettant de définir la synchronisation dans des implémentations Ethernet à 10 Mbits/s et moins rapides. Les versions plus rapides d'Ethernet sont synchrones, aussi ces informations de synchronisation sont-elles inutiles mais conservées à des fins de compatibilité.



Un délimiteur de début de trame (SOF) est constitué d'un champ d'un octet qui marque la fin des informations de synchronisation et qui contient la séquence de bits 10101011.

L'adresse de destination peut être une adresse d'unicast, une adresse de multicast ou une adresse de broadcast.

Le champ d'adresse source contient l'adresse source MAC. Celle-ci est généralement l'adresse d'unicast du nœud Ethernet qui a transmis la trame. Cependant, de nombreux protocoles virtuels utilisent, et parfois partagent, une adresse MAC source afin d'identifier l'entité virtuelle.

Le champ de longueur/type peut être utilisé de deux façons. Si la valeur est inférieure à 1536 en notation décimale, soit 0x600 en notation hexadécimale, alors elle indique la longueur. L'interprétation de la longueur est utilisée lorsque la couche LLC fournit l'identification de protocole. La valeur de type précise le protocole de couche supérieure qui reçoit les données une fois le traitement Ethernet terminé. La longueur indique le nombre d'octets de données qui suit ce champ.

Le champ de données -avec remplissage le cas échéant- peut être de n'importe quelle longueur, pourvu que cela n'entraîne pas un dépassement de la taille maximum de la trame. L'unité de transfert d'informations maximale (MTU) pour Ethernet étant de 1500 octets, les données ne doivent pas dépasser cette taille. Le contenu de ce champ n'est pas spécifié. Une quantité non spécifiée de données est insérée immédiatement après les données utilisateur lorsqu'il n'y a pas suffisamment de données utilisateur pour que la trame ait la longueur minimale. Ces données supplémentaires sont appelées données de remplissage. Ethernet exige que chaque trame ait une longueur comprise entre 64 et 1518 octets.

Une séquence de contrôle de trame (FCS) contient un code de redondance cyclique (CRC) de 4 octets créé par l'unité émettrice et recalculé par l'unité réceptrice afin de s'assurer qu'aucune trame n'a été endommagée. La corruption d'un seul bit, où que ce soit entre le début de l'adresse de destination et la fin du champ FCS, entraînera une différence dans la somme de contrôle. Par conséquent, la séquence de contrôle de trame s'inclut elle-même. Il n'est pas possible de faire la distinction entre la corruption de la FCS et celle d'un autre champ utilisé dans le calcul.

Cette leçon est terminée. La leçon suivante traite des fonctions d'un réseau Ethernet. La première page aborde le concept de MAC.

6.2 Fonctionnement d'Ethernet

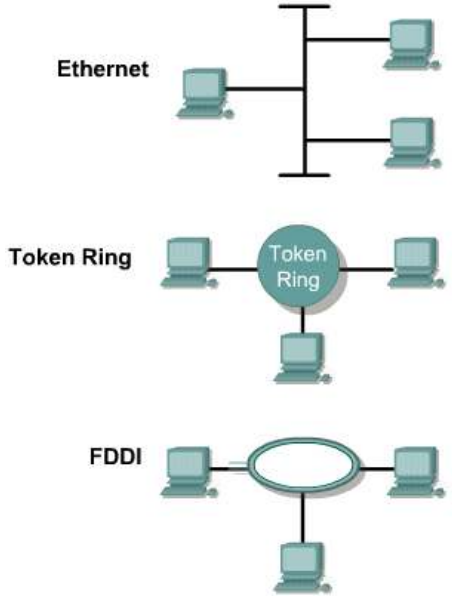
6.2.1 MAC

Cette page définit le MAC et donne des exemples de protocoles MAC déterministes et non déterministes.

L'expression MAC (Media Access Control) fait référence aux protocoles qui, dans un environnement à média partagé (domaine de collision), déterminent l'ordinateur autorisé à transmettre des données. Avec la procédure LLC, la procédure MAC forme la version IEEE de la couche 2, c'est-à-dire qu'elles sont toutes deux des sous-couches de la couche 2. Il y a deux grandes catégories de protocole MAC, l'une déterministe, l'autre non déterministe.

Token Ring et FDDI sont des exemples de protocoles déterministes. Dans un réseau Token Ring, les hôtes sont disposés en anneau et un jeton de données spécial circule d'un hôte à l'autre autour de l'anneau. Lorsqu'un ordinateur hôte désire émettre des données, il saisit le jeton, émet les données pendant un temps limité, puis transmet le jeton à l'hôte suivant sur l'anneau. Token Ring est un environnement dit sans collision, puisqu'un seul hôte peut transmettre à la fois.

Les protocoles MAC non déterministes font appel à la méthode dite du " premier arrivé, premier servi ". Le système CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* ou *détection de porteuse avec accès multiple et détection de collision*) est simple. La carte réseau guette l'absence de signal sur le média, puis commence à transmettre. Si deux nœuds transmettent simultanément, une collision se produit et aucun d'eux n'est alors en mesure de transmettre.



Il existe trois technologies répandues de couche 2 : Token Ring, FDDI et Ethernet. Toutes trois précisent des éléments de couche 2 (par exemple : LLC, attribution de noms, verrouillage de trame et MAC), ainsi que des composants de signalisation et des éléments de média de couche 1. Les technologies utilisées par chacune d'elles

sont les suivantes : 1

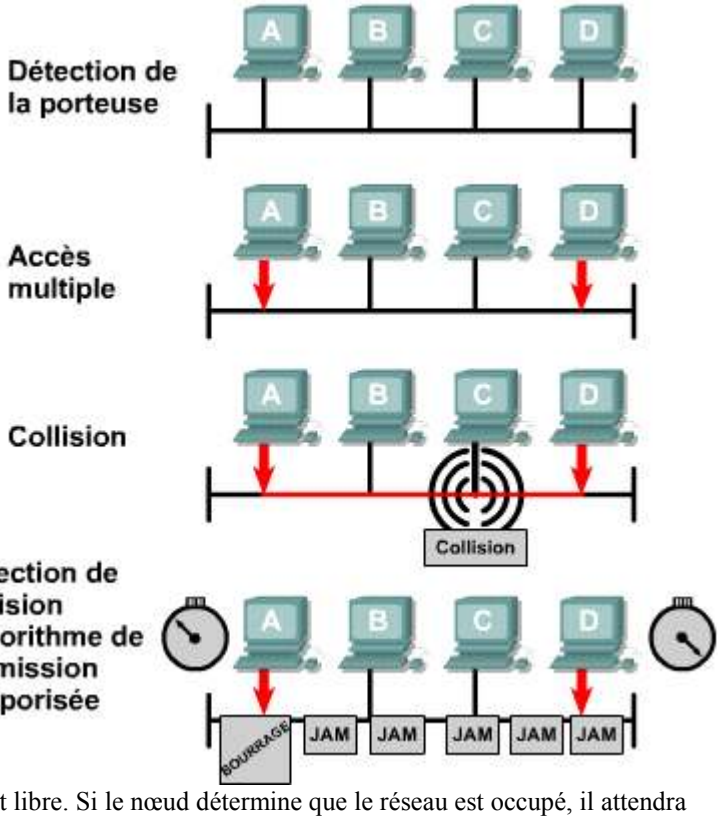
- **Ethernet** – utilise une topologie de bus logique (flux d'informations sur un bus linéaire) et une topologie physique en étoile ou en étoile étendue (câblage en étoile).
- **Token Ring** – utilise une topologie logique en anneau pour contrôler le flux d'informations et une topologie physique en étoile.
- **FDDI** – utilise une topologie logique en anneau pour contrôler le flux d'informations et une topologie physique à deux anneaux.

La page suivante explique comment les collisions sont évitées dans un réseau Ethernet.

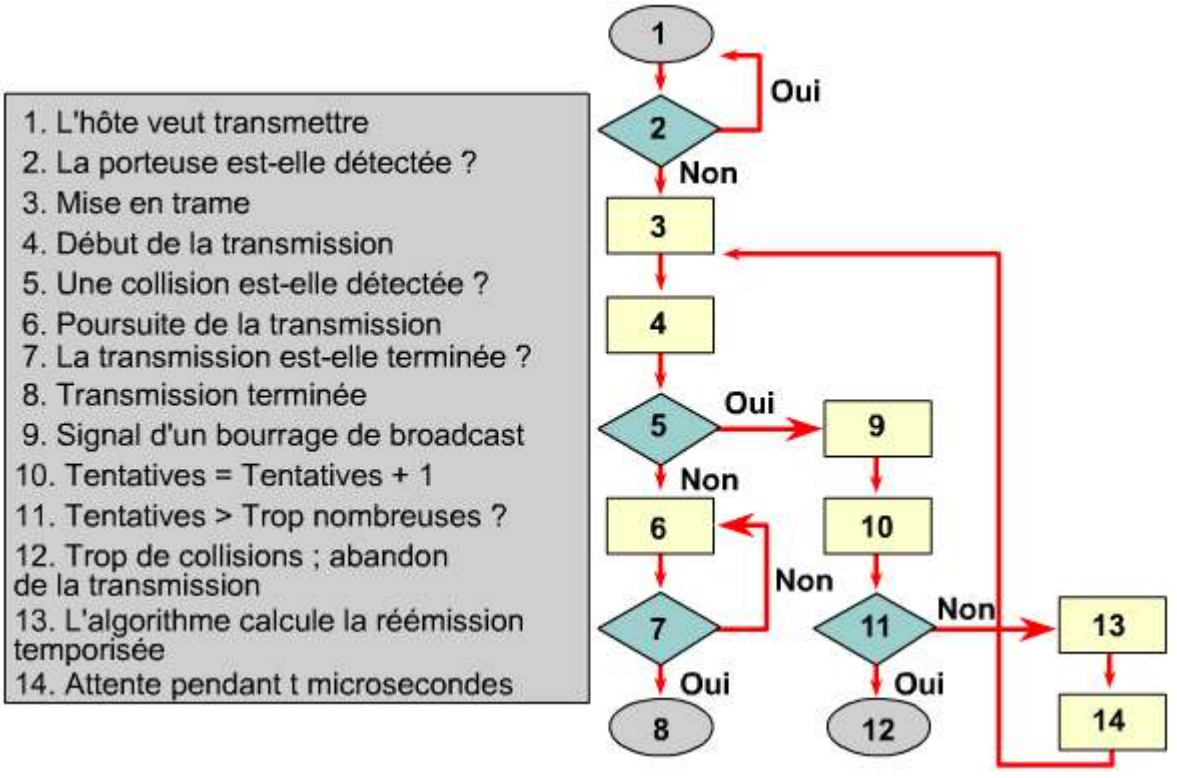
Cette page décrit la détection et la prévention de collision sur un réseau CSMA/CD.

Ethernet est une technologie de broadcast à média partagé. La méthode d'accès CSMA/CD utilisée par le réseau Ethernet remplit les trois fonctions suivantes: 1

- Transmission et réception de trames de données
- Décodage des trames de données et vérification de ces trames afin de s'assurer qu'elles ont une adresse valide avant de les transmettre aux couches supérieures du modèle OSI
- Détection d'erreurs à l'intérieur des trames de données ou sur le réseau



Dans la méthode d'accès CSMA/CD, les équipements de réseau qui ont des données à transmettre sur le média réseau ne le font qu'après écoute de porteuse. Concrètement, cela signifie que lorsqu'un nœud souhaite transmettre des données, il doit d'abord s'assurer que le média réseau est libre. Si le nœud détermine que le réseau est occupé, il attendra pendant une durée aléatoire avant de réessayer. Si le nœud détermine que le média est libre, il commence la transmission et l'écoute. Le nœud se met à l'écoute pour s'assurer qu'aucune autre station ne transmet en même temps. Une fois la transmission de données terminée, l'équipement se remet en mode d'écoute. 2



Les équipements de réseau détectent qu'une collision s'est produite lorsque l'amplitude du signal augmente sur le média réseau. Lorsqu'une collision se produit, chaque nœud émetteur continue de transmettre des données pendant une courte période afin de s'assurer que tous les nœuds détectent la collision. Lorsque tous les nœuds ont détecté la collision, l'algorithme de réémission temporisée est appelé et la transmission s'arrête. Les nœuds arrêtent de transmettre pendant une période aléatoire, déterminée par l'algorithme de réémission temporisée. À l'expiration du délai, chaque nœud peut tenter d'accéder à nouveau au média réseau. Les équipements impliqués dans la collision ne sont pas prioritaires pour la transmission des données.

L'activité de média interactive montre la procédure de détection de collision dans un réseau Ethernet.

La page suivante traite de la synchronisation Ethernet.

Activité de média interactive

Glisser-Positionner: Organigramme de la détection de collisions

À la fin de cette activité, l'étudiant doit être en mesure d'identifier la procédure de détection de collisions sur un réseau Ethernet.

6.2 Fonctionnement d'Ethernet

6.2.3 Synchronisation Ethernet

Cette page explique l'importance des tranches de temps dans un réseau Ethernet.

Les règles et les spécifications de base liées à un fonctionnement approprié d'Ethernet ne sont pas particulièrement complexes, bien que certaines des implémentations de couche physique rapides aient tendance

à le devenir. Malgré cette simplicité élémentaire, lorsqu'un problème se produit sur Ethernet, il est souvent relativement difficile d'en trouver l'origine. En raison de l'architecture de bus commune d'Ethernet, également décrite comme un point de défaillance unique intégré, l'étendue du problème englobe habituellement tous les équipements qui se trouvent dans le domaine de collision. Dans les situations où des répéteurs sont utilisés, cela peut concerner des équipements distants de jusqu'à quatre segments.

Toute station d'un réseau Ethernet qui souhaite transmettre un message " écoute " d'abord pour s'assurer qu'aucune autre station n'est en cours de transmission. Si le câble est silencieux, elle entame immédiatement la transmission. Le signal électrique met un certain temps à parcourir le câble (délai), et chaque répéteur suivant introduit un bref temps de latence lors de la transmission de la trame entre deux ports. En raison du délai et du temps de latence, il est possible pour plusieurs stations de commencer la transmission au même moment ou quasiment au même moment, ce qui engendre une collision.

Si la station connectée fonctionne en mode full duplex, alors elle peut envoyer et recevoir de façon simultanée et les collisions ne doivent pas se produire. Le mode full duplex modifie également les paramètres de synchronisation et élimine le concept de tranche de temps. Le fonctionnement en full duplex permet de concevoir une architecture réseau plus étendue puisque la restriction de synchronisation pour la détection de collisions est éliminée.

En mode half duplex, en supposant qu'aucune collision ne se produise, la station émettrice transmet 64 bits d'informations de synchronisation appelées préambule. La station émettrice transmet alors les informations suivantes:

Informations sur les adresses MAC destination et source

- Certaines autres informations d'en-tête
- Charge utile réelle de données
- Somme de contrôle (FCS) utilisée pour s'assurer que le message n'a pas été corrompu en cours de route

Les stations qui reçoivent la trame recalculent la FCS pour déterminer si le message entrant est valide, puis transmettent les messages valides à la couche supérieure suivante de la pile de protocoles.

Les versions à 10 Mbits/s ou moins d'Ethernet sont asynchrones. Asynchrone signifie que chaque station réceptrice utilisera les huit octets d'informations de synchronisation afin de synchroniser le circuit de réception avec les données entrantes, puis les abandonnera. Les implémentations à 100 Mbits/s et plus d'Ethernet sont synchrones. Synchrone signifie que les informations de synchronisation ne sont pas nécessaires, cependant, pour des raisons de compatibilité le préambule et le délimiteur de début de trame (SFD) sont présents.

Pour toutes les vitesses de transmission Ethernet égales ou inférieures à 1000 Mbits/s, la norme stipule qu'une transmission ne peut pas être inférieure à une tranche de temps. La tranche de temps pour l'Ethernet 10 et 100 Mbits/s est de 512 temps de bit, soit 64 octets. La tranche de temps pour l'Ethernet 1000 Mbits/s est de 4096 temps de bit, soit 512 octets. La tranche de temps est calculée en se basant sur des longueurs de câble maximales dans l'architecture de réseau légale la plus étendue. Tous les délais de propagation sont au maximum légal et le signal de bourrage 32 bits est utilisé lorsque des collisions sont détectées.

La tranche de temps calculée réelle est à peine supérieure à la durée théorique requise pour aller jusqu'aux points les plus éloignés du domaine de collision, entrer en collision avec une autre transmission au dernier moment possible, retourner les fragments de collision à la station émettrice et les détecter. Pour que le système fonctionne, la première station doit détecter la collision avant d'avoir terminé d'envoyer la taille de trame légale la plus petite. Pour permettre à l'Ethernet 1000 Mbits/s de fonctionner en mode half duplex, le champ d'extension a été ajouté aux seules fins d'occuper l'émetteur suffisamment longtemps pour le retour d'un fragment de collision lors de l'envoi de petites trames. Ce champ n'est présent que sur les liaisons 1000 Mbits/s en half duplex et permet aux trames de taille minimale d'être assez longues pour satisfaire aux exigences de tranche de temps. Les bits d'extension sont abandonnés par la station réceptrice.

Sur Ethernet 10 Mbits/s, il faut 100 nanosecondes (ns) pour transmettre un bit au niveau de la couche MAC. À 100 Mbits/s il faut 10 ns pour la transmission de ce bit et donc seulement 1 ns à 1000 Mbits/s. Selon une estimation approximative, la valeur de 20,3 cm par nanoseconde est souvent utilisée pour calculer le délai de propagation le long d'un câble UTP. Pour cent mètres de câble à paires torsadées non blindées, cela signifie qu'il faut 5 temps de bit à peine à un signal 10BaseT pour parcourir la longueur du câble. 1

Vitesse Ethernet	Temps de bit
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

Pour que l'Ethernet CSMA/CD puisse fonctionner, la station émettrice doit avoir connaissance d'une collision avant d'avoir terminé la transmission d'une trame de taille minimum. À 100 Mbits/s, la synchronisation du système est à peine capable de servir 100 mètres de câble. À 1000 Mbits/s, des ajustements spéciaux sont nécessaires du fait qu'environ une trame de taille minimum serait transmise avant que le premier bit n'atteigne la fin des premiers 100 mètres de câble UTP. Pour cette raison, le mode half duplex n'est pas autorisé dans le 10-Gigabit Ethernet.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux identifier le temps de bit des différentes vitesses Ethernet.

La page suivante décrit l'espacement intertrame et la réémission temporisée.



Activité de média interactive

Glisser-Positionner: Synchronisation Ethernet

À la fin de cette activité, l'étudiant doit être en mesure d'identifier les temps de bit des différentes vitesses Ethernet.

6.2 Fonctionnement d'Ethernet

6.2.4 Espacement intertrame et réémission temporisée

Cette page explique comment l'espacement est utilisé dans un réseau Ethernet pour la transmission des données.

L'espacement minimum entre deux trames n'entrant pas en collision est appelé espacement intertrame. Cet espacement a pour limites le dernier bit du champ de la FCS de la première trame et le premier bit du préambule de la deuxième trame.

Vitesse	Espacement intertrame	Temps nécessaire
10 Mbps	96 temps de bit	9.6 µs
100 Mbps	96 temps de bit	0.96 µs
1 Gbps	96 temps de bit	0.096 µs
10 Gbps	96 temps de bit	0.0096 µs

1

Lorsqu'une trame est envoyée, toutes les stations d'un réseau Ethernet 10 Mbits/s doivent attendre au minimum une durée de 96 bits, soit 9,6 microsecondes, avant qu'une autre station ait le droit de transmettre la trame suivante. Sur les versions plus rapides d'Ethernet, l'espacement reste le même, à savoir 96 temps de bit, mais le temps nécessaire pour cet intervalle se réduit de façon proportionnelle. On appelle cet intervalle écart d'espacement. Cet écart est prévu pour donner le temps aux stations lentes de traiter la trame précédente et de se préparer pour la suivante.

Un répéteur doit régénérer les 64 bits d'informations de synchronisation, correspondant au préambule et à la SFD, au début de chaque trame. Cela doit se faire malgré la perte potentielle de certains bits de début de préambule en raison de la lenteur de la synchronisation. À cause de cette réintroduction forcée de bits de synchronisation, une certaine réduction minime de l'écart intertrame est non seulement possible mais attendue. Certains jeux de circuits Ethernet sont sensibles à un raccourcissement de l'espacement intertrame, et risquent de ne plus pouvoir détecter les trames en cas de réduction de l'écart. En raison de l'augmentation de leur puissance de traitement, les ordinateurs personnels pourraient très facilement saturer un segment Ethernet de trafic et commencer à retransmettre avant l'observation du délai d'espacement intertrame.

Lorsque la collision s'est produite et que toutes les stations rendent le câble inactif (en attente de l'espacement intertrame complet), alors les stations à l'origine de la collision doivent observer un délai supplémentaire et potentiellement de plus en plus long avant de tenter de retransmettre la trame entrée en collision. Le délai d'attente est conçu intentionnellement pour être aléatoire afin que les deux stations n'observent pas le même délai avant de retransmettre, ce qui entraînerait d'autres collisions. Pour cela, on étend l'intervalle qui sert de base à la sélection du temps de retransmission lors de chaque tentative de retransmission. La période d'attente est mesurée par incréments de tranche de temps. 2

Vitesse	Tranche de temps	Intervalles de temps
10 Mbps	512 temps de bit	51.2 µs
100 Mbps	512 temps de bit	5.12 µs
1 Gbps	4096 temps de bit	4.096 µs
10 Gbps	non applicable	non applicable

Si la couche MAC est incapable d'envoyer la trame après seize tentatives, elle abandonne et génère une erreur sur la couche réseau. Une telle situation est assez rare et ne peut se produire qu'en cas de surcharge extrême du réseau, ou lorsqu'il existe un problème physique.

La page suivante traite des collisions.

6.2 Fonctionnement d'Ethernet

6.2.5 Traitement des erreurs

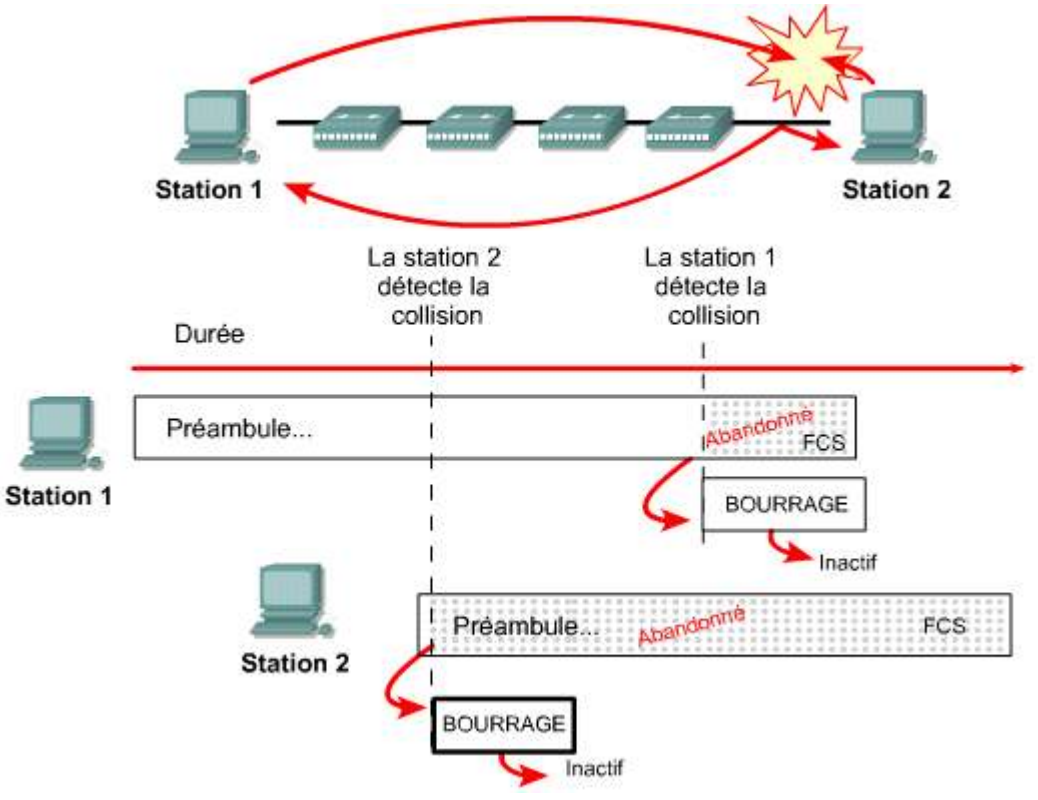
Cette page décrit les collisions et la façon dont elles sont gérées sur un réseau.

La condition d'erreur la plus commune sur les réseaux Ethernet est la collision. 1La collision est le mécanisme qui permet de résoudre un conflit d'accès au réseau. Lorsqu'elles sont peu nombreuses, les collisions constituent pour les nœuds de réseau un moyen simple, rapide et léger en terme de charge administrative, d'arbitrer les conflits d'accès aux ressources réseau. Lorsque le conflit devient trop important, les collisions peuvent devenir de sérieux obstacles pour le fonctionnement effectif du réseau.

Les collisions entraînent une perte de la bande passante réseau qui est équivalente à la transmission initiale et au signal de bourrage de collision. Il s'agit d'un délai de consommation qui affecte tous les nœuds de réseau et qui peut provoquer une réduction significative du débit du réseau.

La grande majorité des collisions se produit au tout début de la trame, souvent avant le délimiteur de début de trame (SFD). Les collisions qui se produisent avant le SFD ne sont généralement pas signalées aux couches supérieures, comme si elles n'avaient pas eu lieu. Dès qu'une collision est détectée, les stations émettrices transmettent un signal de " bourrage " sur 32 bits (jam) qui signale la collision. Cela est effectué afin que toute donnée transmise soit complètement corrompue et que toutes les stations aient une chance de détecter la collision.

Dans la figure 1



, deux stations écoutent pour s'assurer que le câble est inactif, puis elles transmettent. La station 1 a pu transmettre une grande partie de la trame avant que le signal n'atteigne le dernier segment de câble. La station 2 n'avait pas reçu le premier bit de la transmission avant de commencer sa propre transmission et a pu envoyer plusieurs bits avant que sa carte réseau ne décèle la collision. La station 2 a immédiatement tronqué la transmission en cours, remplacé le signal de bourrage 32 bits et mis fin à toutes les transmissions. Au cours de la collision et de l'événement de bourrage subi par la station 2, les fragments de collision ont tenté de retourner à la station 1 en traversant le domaine de collision répété. La station 2 a terminé la transmission du signal de bourrage 32 bits et s'est tue avant que la collision ne se propage vers la station 1 qui ignorait encore la collision et continuait de transmettre. Lorsque les fragments de collision ont finalement atteint la station 1, elle a également tronqué la transmission en cours et substitué un signal de bourrage 32 bits au reste de la trame qu'elle était en train de transmettre. Dès l'envoi du signal de bourrage 32 bits, la station 1 a cessé toute transmission.

Un signal de bourrage peut être constitué de n'importe quelles données binaires, tant qu'il ne forme par une somme de contrôle valide pour la partie de la trame déjà transmise. Le modèle de données le plus communément observé pour un signal de bourrage est simplement un modèle répétitif de un, zéro, un, zéro identique au préambule. Dans un analyseur de protocole, ce modèle s'affiche comme une séquence répétitive de 5 ou A en notation hexadécimale. Les messages corrompus et partiellement transmis sont souvent appelés fragments de collision ou rebuts. Les collisions normales sont d'une longueur inférieure à 64 octets et échouent à la fois au test de longueur minimale et au test de somme de contrôle FCS.

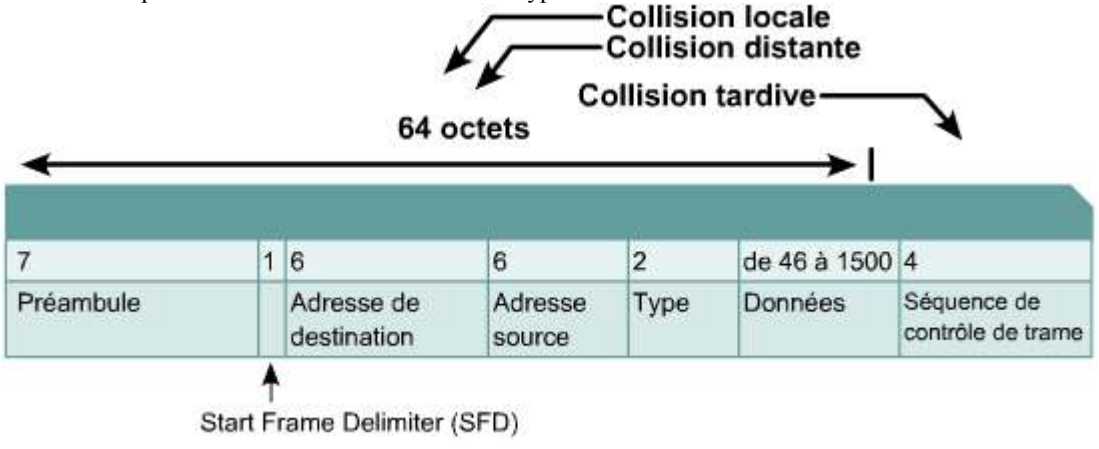
La page suivante définit différents types de collisions.

6.2 Fonctionnement d'Ethernet

6.2.6 Types de collisions

Cette page couvre les différents types de collisions et leurs caractéristiques.

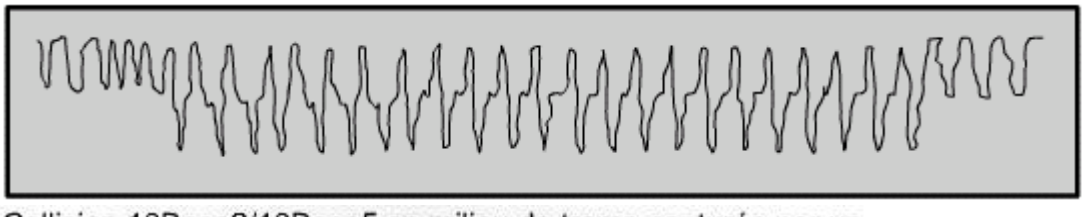
Les collisions se produisent généralement lorsque au moins deux stations Ethernet transmettent simultanément au sein d'un domaine de collision. Une collision unique est une collision qui a été détectée lors d'une tentative de transmission d'une trame, mais qui a abouti à la tentative suivante. On parle de collisions multiples lorsque la même trame est entrée en collision plusieurs fois avant d'être transmise avec succès. Les résultats de collisions et de fragments de collision sont des trames incompatibles ou corrompues qui sont inférieures à 64 octets et comportent une FCS invalide. Les trois types de collision sont les suivants: 1



- Locale
- Distante
- Tardive

Pour créer une collision locale sur du câble coaxial (10Base2 et 10Base5), le signal circule sur le câble jusqu'à ce qu'il rencontre un signal de l'autre station. Les ondes se chevauchent alors, annulant certaines parties du signal ou dédoublant d'autres parties. Le dédoublement du signal élève le niveau de tension de ce dernier au-delà du maximum autorisé. Cette condition de surtension est ensuite ressentie par toutes les stations du segment de câble local comme une collision.

Au début, la forme d'onde de la figure 2 représente des données normales codées Manchester. Quelques cycles plus loin dans l'échantillon, l'amplitude de l'onde se met à doubler. C'est le début de la collision, lorsque les deux formes d'onde se chevauchent. Juste avant la fin de l'échantillon, l'amplitude retourne à la normale. Cela se produit lorsque la première station à détecter la collision arrête de transmettre et que le signal de bourrage de la deuxième station en collision est encore observé. 2



Collision 10Base2/10Base5 en milieu de trame capturée par un oscilloscope à stockage numérique.

Sur un câble UTP, tel que 10BaseT, 100BaseTX et 1000BaseT, une connexion n'est détectée sur le segment local que lorsqu'une station détecte un signal sur la paire réceptrice en même temps qu'il envoie sur la paire émettrice. Puisque les deux signaux sont sur des paires différentes, il n'y a aucune modification caractéristique du signal. Les collisions ne sont reconnues sur du câble UTP que lorsque la station fonctionne en mode half duplex. À ce titre, la seule différence fonctionnelle entre le fonctionnement en mode half duplex et en mode full duplex consiste à savoir s'il est possible ou non d'utiliser de façon simultanée les paires de transmission et de réception. Si la station n'est pas en train de transmettre, elle ne peut pas détecter une collision locale. Réciproquement, une défaillance du câble due à une diaphonie excessive peut faire percevoir à une station sa propre transmission comme une collision locale. Les caractéristiques d'une collision distante sont celles d'une trame de longueur inférieure à la longueur minimum, dont la somme de contrôle FCS est invalide, mais qui ne manifeste pas de signe de collision locale tel qu'une surtension ou une activité de réception/transmission simultanée. Cette sorte de collision résulte habituellement de collisions qui se produisent du côté éloigné d'une connexion répétée. Un répéteur ne transmettra pas un état de surtension, et ne peut pas être à l'origine de l'activité simultanée des paires TX et RX de la station. La station doit être en train de transmettre pour que les deux paires soient actives, ce qui constitue une collision locale. Sur les réseaux UTP, il s'agit d'un type de collision couramment observable.

Il ne reste aucune possibilité pour une collision normale ou légale après que les 64 premiers octets aient été transmis par les stations émettrices. Les collisions qui se produisent après les 64 premiers octets sont appelées "collisions tardives". La différence la plus significative entre les collisions tardives et les collisions qui se produisent avant les 64 premiers octets réside dans le fait que la carte réseau Ethernet retransmettra automatiquement une trame entrée en collision de façon normale, mais ne le fera pas pour une trame dont la collision a été tardive. Au niveau de la carte réseau, tout s'est bien déroulé, et les couches supérieures de la pile de protocoles doivent déterminer que la trame a été perdue. Hormis la retransmission, une station qui détecte une collision tardive la traite exactement de la même façon qu'une collision normale.

Les étudiants peuvent utiliser l'activité de média interactive pour mieux appréhender les différents types de collisions.

La page suivante traite des sources d'erreur Ethernet.



Activité de média interactive

Glisser-Positionner: Types de collisions

À la fin de cette activité, l'étudiant connaîtra les trois différents types de collisions.

6.2 Fonctionnement d'Ethernet

6.2.7 Erreurs Ethernet

Cette page définit les erreurs courantes sur Ethernet.

La connaissance des erreurs types est inestimable pour comprendre le fonctionnement et le dépannage des réseaux Ethernet.

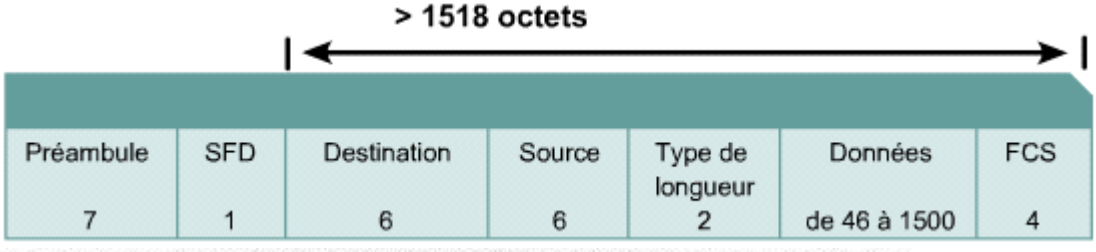
Voici les sources d'erreur types d'Ethernet:

- **Collision ou rebut(runt)** – Transmission simultanée qui se produit avant que la tranche de temps ne se soit écoulée
- **Collision tardive** – Transmission simultanée qui se produit après que la tranche de temps se soit écoulée
- **Jabber, trame longue et erreurs de plage** – Transmission excessivement ou illégalement longue

- **Trame courte, fragment de collision ou runt** – Transmission illégalement courte
- **Erreur FCS** – Transmission corrompue
- **Erreur d'alignement** – Nombre insuffisant ou excessif de bits transmis
- **Erreur de plage** – Le nombre réel et le nombre signalé d'octets de la trame ne correspondent pas
- **Fantôme (ghost) ou longueur excessive (jabber)** – Préambule anormalement long ou événement de bourrage

Alors que les collisions locales et distantes sont considérées comme faisant partie du fonctionnement normal d'Ethernet, les collisions tardives sont considérées comme des erreurs. La présence d'erreurs dans un réseau suggère toujours qu'une investigation plus poussée va suivre. En fonction des erreurs détectées, la gravité du problème détermine l'urgence du dépannage. Ainsi quelques erreurs détectées en plusieurs minutes ou en plusieurs heures seront d'une priorité basse. Par contre, des milliers d'erreurs détectées en quelques minutes relèveront de l'urgence.

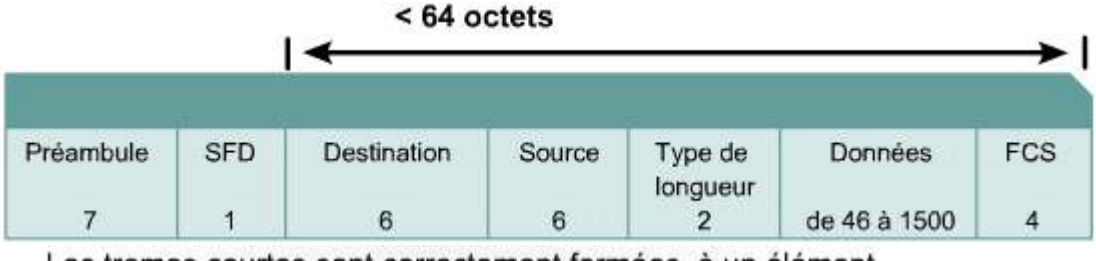
Le jabber est défini dans différentes sections de la norme 802.3 comme une transmission d'une durée d'au moins 20 000 à 50 000 temps de bit. Cependant, la plupart des outils de diagnostic signalent ce type d'erreur chaque fois qu'une transmission détectée dépasse la taille de trame légale maximum, qui est bien inférieure à une durée de 20 000 à 50 000 temps de bit. De façon plus appropriée, on parlera de trames longues plutôt que de jabber. [1]



Les jabbers et les trames longues dépassent la longueur maximale de trame. Les jabbers sont beaucoup plus longs.

Une trame longue est une trame, étiquetée ou non, dont la longueur dépasse la taille légale. Il n'est pas tenu compte du fait que la trame a une somme de contrôle FCS valide. Cette erreur signifie en général que du jabber a été détecté sur le réseau.

Une trame courte est une trame qui est plus petite que la taille minimum légale de 64 octets, et dont la séquence de contrôle de trame est bonne. Certains analyseurs de protocole et moniteurs de réseau appellent ces trames " runts ". En général, la présence de trames courtes ne veut pas dire que le réseau est défaillant.



Les trames courtes sont correctement formées, à un élément près. Elles ont des sommes de contrôle valides, mais leur taille est inférieure à la taille de trame minimale (64 octets).

Le terme de jargon runt désigne en général quelque chose d'inférieur à la taille de trame légale. Il peut se rapporter à des trames courtes dont la somme de contrôle FCS est valide, bien qu'il soit plutôt employé pour les fragments de collision.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les erreurs Ethernet.

La page suivante continue la description des erreurs de trame Ethernet.

Activité de média interactive

Associer: Correspondance des erreurs Ethernet

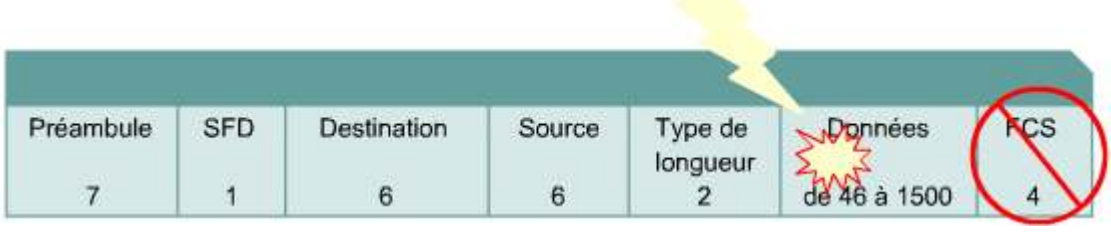
À la fin de cette activité, l'étudiant doit être en mesure de comprendre les termes et définitions relatifs aux erreurs Ethernet.

6.2 Fonctionnement d'Ethernet

6.2.8 Séquence de contrôle de trame et au-delà

Cette page met l'accent sur d'autres erreurs qui se produisent sur un réseau Ethernet.

Une trame reçue dont la séquence de contrôle de trame est mauvaise (également appelée somme de contrôle ou erreur CRC), diffère de la transmission originale d'au moins un bit. Dans une trame FCS erronée, les informations d'en-tête sont probablement correctes, mais la somme de contrôle calculée par la station réceptrice ne correspond pas à celle rattachée à la fin de la trame par la station émettrice. [1]



La trame est alors abandonnée.

Un nombre élevé d'erreurs FCS d'une seule station est habituellement le signe d'une carte réseau défaillante et/ou de pilotes logiciels défaillants ou corrompus, ou encore d'un mauvais câble reliant cette station au réseau. Si les erreurs FCS sont associées à de nombreuses stations, elles sont généralement dues à un mauvais câblage, à une version inappropriée du pilote de la carte réseau, à un port de concentrateur défaillant ou à un bruit induit dans les systèmes de câbles.

On parle d'erreur d'alignement lorsqu'un message ne se termine pas par une frontière entre octets. Plutôt qu'un nombre correct de bits binaires formant des groupements d'octets complets, on observe des bits supplémentaires (moins de huit). Une telle trame est tronquée à la frontière entre octets la plus proche, et une erreur d'alignement est signalée si la somme de contrôle FCS échoue. Cette erreur est souvent due à des pilotes incorrects ou à une collision, et elle s'accompagne fréquemment d'une défaillance de la somme de contrôle FCS.

On parle d'erreur de plage lorsque la valeur du champ de longueur d'une trame ne correspond pas au nombre d'octets réel dénombré dans la trame reçue. Cette erreur apparaît également lorsque la valeur du champ de longueur est inférieure à la taille minimum légale sans remplissage du champ de données. Une erreur similaire, *Out of Range*, est signalée lorsque la valeur du champ de longueur indique une taille de données qui est trop grande pour être légale.

Fluke Networks a inventé le terme fantôme (*ghost*) pour désigner l'énergie (bruit) détectée sur le câble qui semble être une trame, mais à laquelle il manque un SFD valide. Pour être qualifiée de fantôme, la trame doit

être d'une longueur de 72 octets au moins, préambule compris. Sinon, elle entre dans la catégorie des collisions distantes. En raison de la nature particulière des fantômes, il est important de noter que les résultats des tests dépendent grandement de l'endroit du segment où la mesure est effectuée.

Les boucles de mise à la terre et d'autres anomalies de câblage sont habituellement à l'origine du *ghosting*. La plupart des outils de surveillance du réseau ne détectent pas l'existence des fantômes pour la même raison qu'ils ne détectent pas les collisions de préambule. Les outils se fient entièrement à ce que le jeu de circuits leur indique. Les analyseurs de protocole logiciels, de nombreux analyseurs de protocole matériels, les outils de diagnostics portatifs, ainsi que la plupart des sondes de surveillance à distance (RMON) ne détectent pas ces événements.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les termes et définitions d'Ethernet.

La page suivante décrit l'autonégociation.



Activité de média interactive

Case à cocher: Trouver l'erreur Ethernet

À la fin de cette activité, l'étudiant doit être en mesure de comprendre les termes et définitions des erreurs Ethernet.

6.2 Fonctionnement d'Ethernet

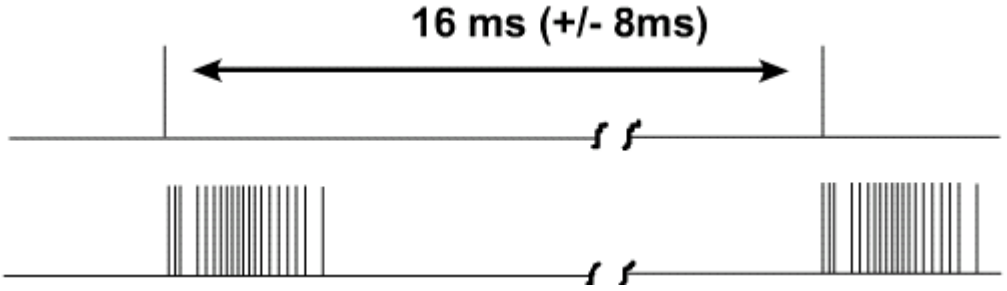
6.2.9 Autonégociation Ethernet

Cette page explique ce qu'est l'autonégociation et la façon dont elle est réalisée.

Lorsque Ethernet est passé de 10 à 100, puis à 1000 Mbits/s, il est devenu nécessaire de rendre chaque technologie interopérable, au point de pouvoir connecter directement les interfaces 10, 100 et 1000. Un processus appelé autonégociation des vitesses en half duplex ou full duplex a été développé. Plus particulièrement, au moment où Fast Ethernet a été introduite, la norme incluait une méthode permettant de configurer de façon automatique une interface donnée afin de l'adapter à la vitesse et aux capacités du partenaire de liaison. Ce processus indique comment deux partenaires de liaison peuvent négocier automatiquement une configuration offrant le meilleur niveau de performances communes. Il présente l'avantage supplémentaire de n'impliquer que la partie inférieure de la couche physique.

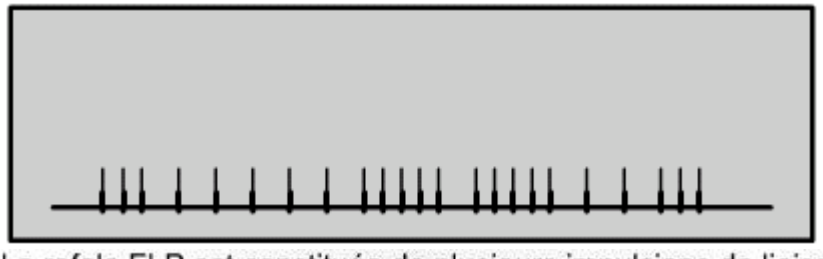
La norme 10BaseT exigeait que chaque station transmette une impulsion de liaison toutes les 16 millisecondes environ, c'est-à-dire à chaque fois que la station n'était pas engagée dans la transmission d'un message. L'autonégociation a adopté ce signal et l'a renommé impulsion de liaison normale (NLP). Lorsqu'une série de NLP est envoyée en groupe à des fins d'autonégociation, ce groupe est appelé rafale FLP (impulsion de liaison rapide). Chaque rafale FLP est envoyée selon le même intervalle de synchronisation qu'une NLP, et elle est conçue pour permettre à des équipements 10BaseT anciens de fonctionner normalement en cas de réception

d'une rafale FLP. 1



L'autonégociation est effectuée en transmettant une rafale d'impulsions de liaison 10BaseT émise par chacun des deux partenaires de liaison. La rafale communique les capacités de la station émettrice à son partenaire de liaison. Après avoir interprété ce que lui propose son partenaire, chaque station bascule sur la configuration commune la plus performante et établit une liaison à cette vitesse. Si un incident quelconque interrompt les communications et que la liaison est perdue, les deux partenaires de liaison tentent en premier lieu d'établir une nouvelle fois la liaison à la vitesse qu'ils avaient négociée en dernier. Si cette tentative échoue, ou si la liaison a été perdue depuis trop longtemps, le processus d'autonégociation recommence. La liaison peut être perdue en raison de facteurs externes, telles qu'une défaillance de câble ou une réinitialisation émise par l'un des partenaires de liaison.

La page suivante aborde les modes half duplex et full duplex.



La rafale FLP est constituée de plusieurs impulsions de liaison NLP

6.2 Fonctionnement d'Ethernet
6.2.10 Établissement de liaison et modes full duplex et half duplex

Cette page explique comment les liaisons sont établies à travers l'autonégociation et présente les deux modes duplex.

Les partenaires de liaison sont autorisés à ignorer l'offre de configuration pour laquelle ils sont équipés. Cela permet à l'administrateur réseau de forcer des ports à une configuration de vitesse et de mode duplex donnée, sans désactiver l'autonégociation.

L'autonégociation est optionnelle pour la plupart des implémentations Ethernet. Gigabit Ethernet requiert sa mise en œuvre, bien que l'utilisateur puisse la désactiver. L'autonégociation a été définie à l'origine pour les implémentations UTP d'Ethernet, et elle a été étendue pour fonctionner avec d'autres implémentations à fibre optique.

Lorsqu'une station d'autonégociation tente pour la première fois d'établir une liaison, elle est supposée activer 100BaseTX pour tenter d'établir une liaison de façon immédiate. En présence de la signalisation 100BaseTX, et si la station prend en charge 100BaseTX, elle tentera d'établir une liaison sans négocier. Si la signalisation produit une liaison ou en cas de réception de rafales FLP, la station poursuivra avec cette technologie. Si un partenaire de liaison ne propose pas de rafale FLP, mais des NLP, cet équipement est automatiquement supposé

être une station 10BaseT. Durant l'intervalle initial de recherche d'autres technologies, le chemin de transmission envoie des rafales FLP. La norme n'autorise la détection parallèle d'aucune autre technologie.

Si une liaison est établie au moyen de la détection parallèle, elle doit obligatoirement se faire en half duplex. Il existe seulement deux méthodes pour réaliser une liaison full duplex. L'une d'elle consiste à effectuer un cycle complet d'autonégociation, et l'autre à forcer administrativement les partenaires de liaison au full duplex. Si l'un des partenaires est forcé à se configurer en full duplex, mais que l'autre tente d'autonégocier, il y a nécessairement un décalage dans le duplex. Cela entraîne des collisions et des erreurs sur cette liaison. De plus, si une extrémité est forcée au mode full duplex, l'autre doit l'être aussi. Le 10-Gigabit Ethernet qui ne prend pas en charge le mode half duplex est une exception.

De nombreux fournisseurs mettent en œuvre le matériel de façon à ce qu'il balaie successivement les divers états possibles. Il transmet des rafales FLP pour autonégocier pendant un moment, puis il se configure pour Fast Ethernet, tente d'établir la liaison pendant un moment, et enfin se met à l'écoute. Certains fournisseurs ne proposent aucune tentative d'établir la liaison jusqu'à ce que l'interface entende une rafale FLP ou un autre schéma de signalisation.

Il y a deux modes duplex, le mode half duplex et le mode full duplex. Le mode half duplex est obligatoire pour les médias partagés. Toutes les implémentations coaxiales sont en half duplex par nature et ne peuvent pas fonctionner en full duplex. Les implémentations UTP et en fibre optique peuvent fonctionner en half duplex. Les implémentations en 10 Gbits/s sont spécifiées pour le full duplex uniquement.

En half duplex, une seule station peut transmettre à la fois. Pour les implémentations coaxiales, la transmission d'une deuxième station entraîne le chevauchement et l'altération des signaux. Puisque le câble UTP et la fibre optique transmettent généralement sur des paires séparées, les signaux ne peuvent se chevaucher ou s'altérer. Ethernet a établi des règles d'arbitrage pour résoudre les conflits engendrés par des situations où plusieurs stations tentent de transmettre en même temps. Les deux stations d'une liaison point-à-point en mode full duplex sont autorisées à transmettre à n'importe quel moment, que l'autre station soit en transmission ou non.

L'autonégociation permet d'éviter la plupart des situations où une station d'une liaison point-à-point transmet en half duplex et l'autre en full duplex.

Pour le cas où les partenaires de liaison ont la possibilité de partager plus d'une technologie, reportez-vous à la liste de la figure 1



La liste est classée par ordre de priorité, en commençant par la configuration de liaison la plus adéquate.

Cette liste sert à déterminer quelle technologie doit être choisie parmi les configurations proposées.

Les implémentations Ethernet à fibre optique ne figurent pas dans cette liste de résolution prioritaire car l'électronique et l'optique de l'interface ne se prêtent pas à une reconfiguration facile entre implémentations. Il est supposé que la configuration de l'interface est fixe. Si les deux interfaces sont en mesure d'autonégocier, c'est qu'elles utilisent déjà les mêmes implémentations Ethernet. Cependant, il reste quelques choix de

configuration à déterminer, tels que la configuration duplex, ou le choix de la station qui jouera rôle de station maître à des fins de synchronisation.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec l'opération d'établissement de liaison.

Cette leçon est terminée. La page suivante récapitule les principaux points évoqués au cours de ce module.



Activité de média interactive

Glisser-Positionner: Organigramme d'établissement de la liaison

À la fin de cette activité, l'étudiant doit être en mesure d'identifier la priorité dans le processus d'établissement d'une liaison.

Résumé

Cette page récapitule les thèmes abordés tout au long du module.

Ethernet n'est pas une technologie réseau unique, mais une famille de technologies de réseau local qui incluent l'existant, Fast Ethernet et Gigabit Ethernet. Lorsque Ethernet doit être étendu pour ajouter un nouveau média ou une nouvelle capacité, l'IEEE publie un nouveau supplément à la norme 802.3. Les nouveaux suppléments reçoivent une désignation d'une ou deux lettres (p. ex. 802.3u). Ethernet repose sur la signalisation de bande de base, qui utilise la totalité de la bande passante du média de transmission. Ethernet fonctionne sur deux couches du modèle OSI, à savoir la moitié inférieure de la couche liaison de données, que l'on appelle sous-couche MAC, et la couche physique. Sur la couche 1, Ethernet comprend l'interfaçage avec les médias, les signaux, les trains binaires se déplaçant sur les médias, les composants qui envoient des signaux sur les médias, ainsi que diverses topologies. Les bits de couche 1 ont besoin d'une structure pour que les trames de la couche 2 OSI puissent être utilisées. La sous-couche MAC de la couche 2 détermine le type de trame approprié pour le média physique.

L'une des points communs à toute les formes d'Ethernet est la structure de trame. C'est ce qui permet aux différents types d'Ethernet de fonctionner ensemble.

Voici plusieurs des champs autorisés ou obligatoires d'une trame Ethernet 802.3:

- Préambule
- Délimiteur de début de trame
- Adresse de destination
- Adresse source
- Longueur/Type
- Données et remplissage
- Séquence de contrôle de trame

Dans les versions 10 Mbits/s et plus lentes d'Ethernet, le préambule fournit les informations de synchronisation dont le nœud récepteur a besoin pour interpréter les signaux électriques qu'il reçoit. Le délimiteur de début de trame marque la fin des informations de synchronisation. Les versions à 10 Mbits/s et plus lentes d'Ethernet sont asynchrones, c'est-à-dire qu'elles utilisent les informations de synchronisation du préambule pour synchroniser le circuit de réception avec les données entrantes. Les implémentations à 100 Mbits/s et plus rapides d'Ethernet sont synchrones. Synchrone signifie que les informations de synchronisation ne sont pas nécessaires, mais pour des raisons de compatibilité, le préambule et le délimiteur de début de trame (SFD) sont quand même présents.

Les champs d'adresse de la trame Ethernet contiennent des adresses de couches 2 ou MAC.

Toutes les trames sont sujettes à des erreurs de causes diverses. Le champ de la séquence de contrôle de trame (FCS) contient un nombre, calculé par le nœud source, qui repose sur les données contenues dans la trame. Lorsqu'il parvient à destination, il est recalculé et comparé afin de vérifier que les données reçues sont complètes et exemptes d'erreur.

Une fois les données tramées, la sous-couche MAC (Media Access Control) est également en charge de déterminer quel ordinateur dans un environnement à média partagé ou domaine de collision, est autorisé à transmettre des données. Il existe deux grandes catégories de MAC, déterministe (chacun son tour) et non déterministe (premier arrivé, premier servi).

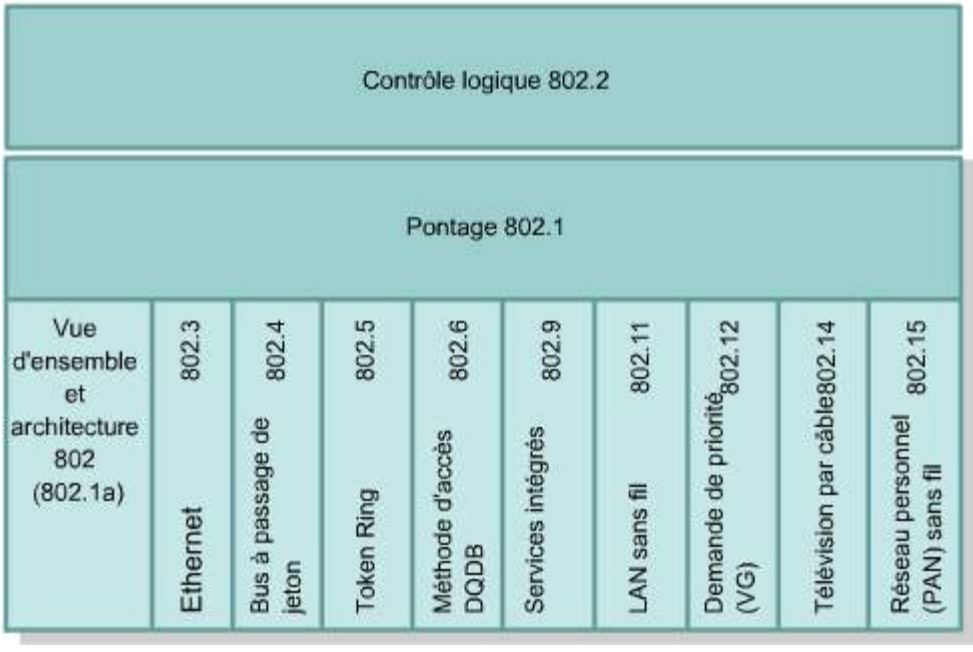
Comme exemple de protocole déterministe, citons Token Ring et FDDI. Le mode de détection de porteuse avec accès multiple et détection de collision (CSMA/CD) est un système non déterministe simple. La carte réseau guette l'absence de signal sur le média, puis commence à transmettre. Si deux nœuds ou plus transmettent simultanément, une collision se produit. Si une collision est détectée, les nœuds attendent pendant une durée aléatoire puis retransmettent.

L'espacement minimum entre deux trames n'entrant pas en collision est appelé espacement intertrame. Cet espacement est nécessaire pour donner le temps à toutes les stations de traiter la trame précédente et de se préparer pour la suivante.

Les collisions peuvent se produire à divers stades de la transmission. On appelle collision locale une collision où un signal est détecté sur les circuits de réception et de transmission en même temps. On appelle collision distante une collision qui se produit avant que le nombre minimal d'octets ait pu être transmis. Une collision qui se produit après que les 64 premiers octets de données ont été envoyés est considérée comme une collision tardive. La carte réseau n'effectue pas de retransmission pour ce type de collision.

Alors que les collisions locales et distantes sont considérées comme des événements normaux du fonctionnement d'Ethernet, les collisions tardives sont considérées comme des erreurs. Les erreurs Ethernet résultent de la détection de trames de longueur supérieure ou inférieure à la norme, ou à des transmissions trop longues ou illégales, appelées jabber. Runt est un terme de jargon qui désigne tout élément inférieur à la taille de trame légale.

L'autonégociation détecte la vitesse de transmission et le mode duplex (half duplex ou full duplex) de l'équipement raccordé à l'autre extrémité du câble, et s'ajuste en fonction de cette configuration.


Contrôle logique 802.2
Pontage 802.1
Vue d'ensemble et architecture 802 (802.1a)
802.3 Ethernet
802.4 Bus à passage de jeton
802.5 Token Ring
802.6 Méthode d'accès DQDB
802.9 Services intégrés
802.11 LAN sans fil
802.12 Demande de priorité (VG)
802.14 Télévision par câble
802.15 Réseau personnel (PAN) sans fil

7-Thechnologies ethernet

Vue d'ensemble

Ethernet est la plus populaire des technologies LAN, principalement en raison de la facilité de sa mise en œuvre. Cette réussite est également due à sa flexibilité, qui lui a permis d'évoluer en fonction des besoins et des capacités des médias. Ce module présente de façon détaillée les principaux types de réseaux Ethernet. L'objectif est de permettre aux étudiants de déterminer les points communs à toutes les formes de ce réseau.

Les modifications apportées au réseau Ethernet ont considérablement amélioré le réseau Ethernet 10 Mbits/s du début des années 80. La technologie Ethernet 10 Mbits/s standard n'a pratiquement pas évolué jusqu'en 1995, lorsque l'IEEE a présenté une norme pour un réseau Fast Ethernet 100 Mbits/s. Ces dernières années, l'évolution de la vitesse des médias s'étant encore accrue, la technologie Gigabit Ethernet a supplanté Fast Ethernet. Et il n'aura fallu que trois ans pour voir apparaître les normes associées à cette nouvelle technologie. Une version Ethernet plus rapide, appelée «10 Gigabit Ethernet», est maintenant largement disponible, et des versions permettant des débits encore plus élevés vont être élaborées.

Les adresses MAC, le réseau CSMA/CD et le format de la trame n'ont pas évolué depuis les premières versions de la technologie Ethernet. Cependant, d'autres aspects de la sous-couche MAC, de la couche physique et du support ont été perfectionnés. Les cartes réseau à base de cuivre de 10, 100 ou 1 000 Mbits/s sont désormais très répandues. Les commutateurs Gigabit et les ports de routeurs deviennent la norme dans les locaux techniques. La fibre optique permettant de prendre en charge la technologie Gigabit Ethernet s'est généralisée pour les câbles de backbone dans la plupart des nouvelles installations.

Ce module se rapporte à des objectifs spécifiques des examens de certification CCNA 640-801, INTRO 640-821 et ICND 640-811. 2

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Description des propriétés et des normes physiques, électriques et mécaniques associées aux médias cuivre, optiques et sans fil utilisés dans les réseaux • Description des problèmes physiques et de topologie associés au câblage des LAN les plus courants • Description des principes et de la mise en pratique de la commutation dans un réseau Ethernet • Explication des concepts fondamentaux associés à la technique d'accès au média Ethernet

À l'issue de ce module, les étudiants seront en mesure d'effectuer les actions suivantes: 1

À la fin de ce chapitre, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
7.1	Ethernet 10 Mbits/s et 100 Mbits/s
7.2	Gigabit et 10 Gigabit Ethernet

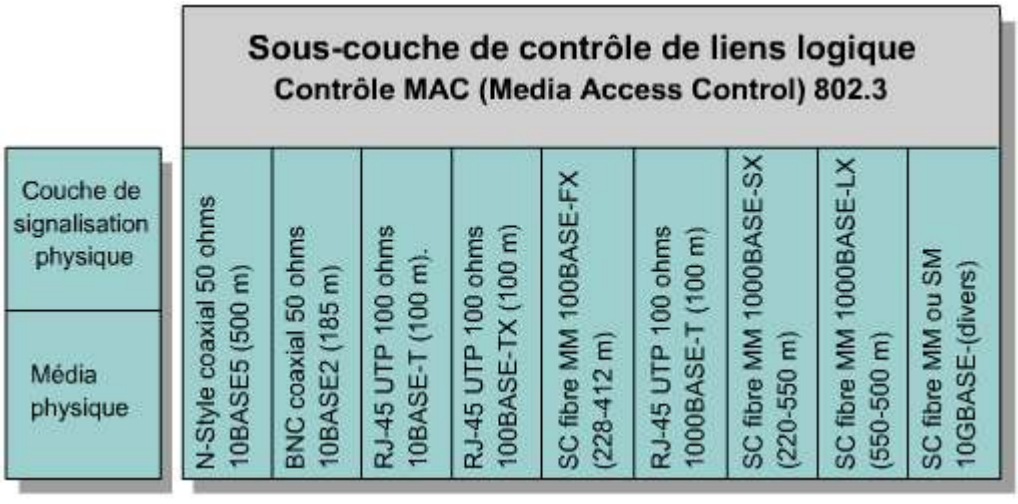
- Décrire les différences et les points communs entre 10BASE5, 10BASE2 et 10BASE-T Ethernet.
- Définir le codage Manchester.
- Énumérer les facteurs qui affectent les délais d'un réseau Ethernet.
- Énumérer les paramètres du câblage 10BASE-T.
- Décrire les principales caractéristiques et variétés d'un réseau Ethernet 100 Mbits/s.
- Décrire l'évolution d'Ethernet.
- Expliquer les méthodes MAC, les formats de trame et le processus de transmission de Gigabit Ethernet.
- Décrire les utilisations de médias et de codage spécifiques avec la technologie Gigabit Ethernet.
- Identifier les broches et le câblage propres aux différentes mises en œuvre de Gigabit Ethernet.
- Décrire les différences et les points communs entre les technologies Gigabit et 10 Gigabit Ethernet.
- Présenter les considérations de base relatives à l'architecture des technologies Gigabit et 10 Gigabit Ethernet.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.1 Ethernet 10 Mbits/s

Cette page décrit les technologies Ethernet de 10 Mbits/s.

Les technologies Ethernet 10BASE5, 10BASE2 et 10BASE-T sont considérées comme les versions initiales d'Ethernet. 1


Sous-couche de contrôle de liens logique
Contrôle MAC (Media Access Control) 802.3
Couche de signalisation physique
Média physique
N-Style coaxial 50 ohms 10BASE5 (500 m)
BNC coaxial 50 ohms 10BASE2 (185 m)
RJ-45 UTP 100 ohms 10BASE-T (100 m).
RJ-45 UTP 100 ohms 100BASE-TX (100 m)
SC fibre MM 100BASE-FX (228-412 m)
RJ-45 UTP 100 ohms 1000BASE-T (100 m)
SC fibre MM 1000BASE-SX (220-550 m)
SC fibre MM 1000BASE-LX (550-500 m)
SC fibre MM ou SM 10GBASE-(divers)

Elles ont en commun quatre caractéristiques, à savoir les paramètres de synchronisation, le format de la trame, les processus de transmission et la règle de conception de base.

La figure 2

Paramètre	Valeur
Durée d'un bit	100 nanosecondes (ns)
Durée d'une tranche	Durée de 512 bits (64 octets)
Espacement intertrame	96 bits *
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)

* La valeur indiquée correspond à l'espacement officiel intertrame. Lorsqu'une trame est envoyée, toutes les stations d'un réseau Ethernet 10 Mbits/s doivent attendre au minimum une durée de 96 bits, soit 9,6 microsecondes, avant qu'une autre station transmette la trame suivante.

présente les paramètres d'Ethernet 10 Mbits/s. Ethernet 10 Mbits/s et les versions plus lentes sont asynchrones. Chaque station de réception utilise huit octets d'informations sur la synchronisation afin de synchroniser son circuit de réception avec les données entrantes. Les technologies 10BASE5, 10BASE2 et 10BASE-T disposent toutes des mêmes paramètres de synchronisation. Exemple : durée d'un bit à 10 Mbits/s = 100 nanosecondes (ns) = 0,1 microseconde = un dix millionième de seconde. Cela signifie que sur un réseau Ethernet de 10 Mbits/s, le transfert d'un bit au niveau de la sous-couche MAC dure 100 ns.

Pour toutes les vitesses de transmission Ethernet de 1 000 Mbits/s ou plus lentes, la transmission ne peut pas dépasser la durée définie. Cette durée est supérieure au temps théoriquement nécessaire pour aller d'une extrémité à l'autre du domaine de collision Ethernet traditionnel le plus important, entrer en collision avec une autre transmission au tout dernier instant et renvoyer les fragments de collision à la station émettrice afin d'être détectés.

Les normes 10BASE5, 10BASE2 et 10BASE-T présentent aussi le même format de trame. 3

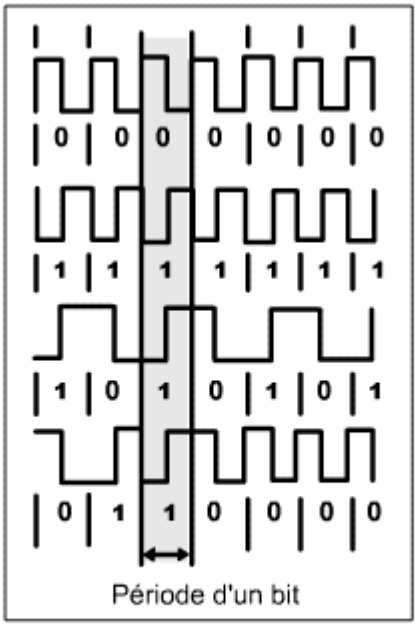
Trame Ethernet						
Préambule	SFD	Destination	Source	Type de longueur	Données Bourrage	FCS
7	1	6	6	2	De 46 à 1 500	4

Le processus de transmission de la version Ethernet initiale est identique jusqu'à la partie inférieure de la couche physique OSI. Lorsque la trame passe de la sous-couche MAC à la couche physique, d'autres processus se produisent avant que les bits ne soient déplacés de la couche physique vers le support. Le signal d'erreur de qualité de ligne est un processus important. Il s'agit d'une transmission renvoyée au contrôleur par un émetteur-récepteur pour lui indiquer si les circuits de collision sont opérationnels. Ce signal d'erreur est également appelé « pulsation ». Il est destiné à résoudre le problème qui se produit dans les versions précédentes d'Ethernet lorsqu'un hôte ne sait pas si un émetteur-récepteur est connecté. Ce signal est toujours utilisé en half-duplex. Son utilisation en full duplex est possible, mais pas indispensable. Il est actif dans les cas suivants:

- Dans un délai de 4 à 8 microsecondes après une transmission normale pour indiquer que la trame de sortie a été correctement transmise.
- En cas de collision sur le support.
- en cas de signal incorrect sur le support, tel qu'une erreur de message trop long, ou de réflexion due à un court-circuit.
- Lorsqu'une transmission a été interrompue.

Toutes les formes Ethernet de 10 Mbits/s récupèrent les octets provenant de la sous-couche MAC et lancent un processus appelé « codage de ligne ». Le codage de ligne décrit le type de signalement des bits sur le câble. Le codage le plus simple comporte des caractéristiques de synchronisation et des propriétés électriques qui ne sont pas adaptées. Par conséquent, les codes de ligne ont été élaborés avec des propriétés de transmission plus appropriées. Cette forme de codage utilisée dans les systèmes de 10 Mbits/s est appelée «codage Manchester».

Le codage Manchester utilise la transition au milieu de la fenêtre de synchronisation pour déterminer la valeur binaire de cette période de bits. Pour le premier exemple de la figure 4



Voici un exemple de codage Manchester. L'axe des y représente la tension. L'axe des x représente la durée.

, la valeur du signal transite vers une valeur inférieure et est alors interprétée en tant que zéro binaire. Pour le deuxième exemple, la valeur du signal transite vers une valeur plus élevée et est interprétée en tant que 1 binaire. Le troisième exemple présente une séquence binaire en alternance. Lorsque les données binaires alternent, il n'est pas nécessaire de revenir au voltage précédent avant la période de bits suivante. Les ondes du graphique indiquent que les valeurs de bits binaires sont déterminées d'après le sens de la modification dans une période de bits. Les niveaux de voltage au début et à la fin d'une période de bits ne sont pas utilisés pour déterminer les valeurs binaires.

Les caractéristiques de l'architecture des technologies Ethernet initiales présentent plusieurs points communs. Les réseaux comportent généralement plusieurs types de médias. La norme permet de garantir l'interopérabilité. La conception générale de l'architecture est plus importante dans les réseaux de médias mixtes. Il est en effet plus facile de dépasser les délais maximums lorsque le réseau devient étendu. La synchronisation est fonction des types de paramètres suivants:

- La longueur de câble et le délai de propagation.
- Le délai des répéteurs.
- Le délai des émetteurs-récepteurs.
- La réduction des vides intertrames.
- Les délais au sein de la station.

La fenêtre temporelle de la technologie Ethernet de 10 Mbits/s se caractérise par un ensemble pouvant comprendre jusqu'à cinq segments séparés par un maximum de quatre répéteurs. Cette règle est appelée « règle 5-4-3 ». Ces ensembles ne peuvent pas utiliser plus de quatre répéteurs entre deux stations. De même, trois segments maximum peuvent être remplis entre deux stations.

La page suivante présente la technologie 10BASE5.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.2 10BASE5

Cette page présente le produit Ethernet d'origine, développé en 1980: 10BASE5. Ce produit transmettait 10 Mbits/s sur un bus à câble coaxial unique.

Son intérêt réside dans le fait qu'il a été le premier support utilisé pour Ethernet. Il a également été inclus dans la norme 802.3 d'origine. Le principal avantage du câble 10BASE5 était sa longueur. On le trouve encore dans les anciennes installations. Il n'est pas recommandé pour les nouvelles installations. Les systèmes 10BASE5 sont peu onéreux et ne nécessitent aucune configuration. Ils présentent toutefois deux inconvénients : les composants de base tels que les cartes réseau sont très difficiles à trouver et ils sont sensibles à la réflexion des signaux sur le câble. Les systèmes 10BASE5 constituent également un point de défaillance unique.

Ils utilisent le codage Manchester et comportent un conducteur central rigide. Chaque segment de câble coaxial épais peut avoir une longueur de 500 m. Le câble est large, lourd et difficile à installer. Cependant, les limitations sur la distance d'utilisation étaient favorables et cela a prolongé son utilisation dans certaines applications.

Lorsque le support est un câble coaxial unique, une seule station à la fois peut effectuer un transfert, afin d'éviter tout risque de collision. Par conséquent, les systèmes 10BASE5 fonctionnent uniquement en mode half-duplex avec un débit maximum de 10 Mbits/s.

La figure 1 illustre une configuration d'un domaine de collision de bout en bout avec le nombre maximum de segments et de répéteurs. N'oubliez pas que seuls trois segments peuvent être connectés à des stations. Les deux autres segments répétés sont utilisés pour étendre le réseau.

L'activité de TP permet aux étudiants de décoder une onde.

L'activité de média interactive vous aidera à vous familiariser avec les fonctions de la technologie 10BASE5.

La page suivante présente la technologie 10BASE2.

Activité de TP

Exercice: Décodage d'une onde

L'objectif de ce TP est d'appréhender ce que sont les médias réseau, les couches OSI 1, 2 et 3 ainsi qu'Ethernet. Pour ce faire, nous allons décoder l'onde numérique d'une trame Ethernet.

Activité de média interactive

Associer: 10BASE5

À l'issue de cette activité, les étudiants connaîtront les caractéristiques de la technologie 10BASE5.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.3 10BASE2

Cette page traite de la technologie 10BASE2, présentée en 1985.

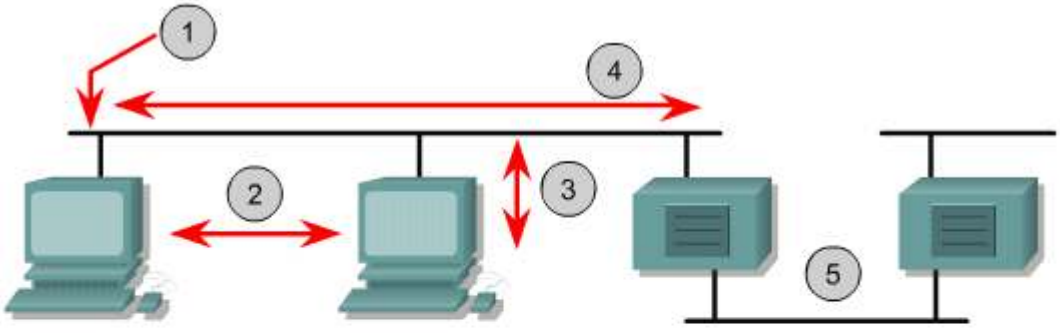
Son installation a été plus facile en raison de la taille réduite du système. Il est également plus léger et plus flexible. La technologie 10BASE2 est toujours employée dans les réseaux existants. À l'instar de la technologie 10BASE5, cependant, elle n'est plus recommandée. Il s'agit d'un système peu coûteux et qui ne requiert pas de concentrateur.

10BASE2 fait également appel au codage Manchester. Les ordinateurs qui ont recours à un LAN de type 10BASE2 sont liés entre eux par une série ininterrompue de câbles coaxiaux. Ces câbles sont reliés à un connecteur en T de la carte réseau, avec des connecteurs BNC.

Les systèmes 10BASE2 comportent un conducteur central torsadé. Chacun des cinq segments d'un câble coaxial fin peut atteindre 185 m de long et chaque station est directement connectée au connecteur BCN en T du câble coaxial.

Une seule station à la fois peut transmettre, sous peine de collision. Les systèmes 10BASE2 utilisent aussi le mode half-duplex. Leur débit maximal est de 10 Mbits/s.

Un segment 10BASE2 peut comporter jusqu'à 30 stations. Seuls trois des cinq segments consécutifs entre deux stations peuvent être remplis. [1]



1. La résistance de terminaison à chaque extrémité du câble coaxial doit être de 50 ohms.
2. La distance minimum entre les "Té" est de 0,5 mètre.
3. Chaque station doit être raccordée à quatre centimètres maximum du câble coaxial fin.
4. La longueur maximale du segment est de 185 mètres.
5. Les segments de liaison entre les répéteurs ne doivent pas avoir plus de deux connexions, les répéteurs eux-mêmes.

L'activité de média interactive vous aidera à vous familiariser avec les fonctions de la technologie 10BASE2.

La page suivante présente la technologie 10BASE-T.

Activité de média interactive

Associer: 10BASE2

À l'issue de cette activité, les étudiants connaîtront les caractéristiques de la technologie 10BASE2.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.4 10BASE-T

Cette page traite de la technologie 10BASE-T, présentée en 1990.

La technologie 10BASE-T utilisait plutôt des câbles en cuivre UTP de catégorie 3 et non des câbles coaxiaux. Ce type de câble était en effet moins onéreux et plus facile à installer. Le câble était relié à une unité de connexion centrale qui contenait le bus partagé. Cette unité était un concentrateur. Ce dernier était au centre d'un ensemble de câbles reliés aux ordinateurs, tels les rayons d'une roue. C'est ce qu'on appelle la topologie en étoile. Avec l'ajout d'ordinateurs et l'augmentation des distances, la topologie en étoile étendue est apparue. À l'origine, le système 10BASE-T était un protocole half-duplex, mais des fonctionnalités full duplex ont été ajoutées ultérieurement. La forte popularité qu'ont connue les réseaux Ethernet entre le milieu et la fin des années 1990 a eu lieu lorsqu'Ethernet a supplanté la technologie LAN.

Les systèmes 10BASE-T utilisent également le codage Manchester. Un câble UTP 10BASE-T comporte un conducteur rigide pour chaque fil. La longueur maximale de câble est de 90 m. Le câble UTP utilise des connecteurs RJ-45 à huit broches. Bien que le câble de catégorie 3 soit adapté aux réseaux 10BASE-T, les nouvelles installations doivent utiliser des câbles de catégorie 5e ou supérieure. L'ensemble des quatre paires de fils doit être associé à des broches T568A ou T568B. Ce type de câblage prend en charge l'utilisation de plusieurs protocoles sans qu'un nouveau câblage soit nécessaire. La figure 1

Nombre de broches	Signal
1	TD+ (Envoi de données, signal différentiel positif)
2	TD- (Envoi de données, signal différentiel négatif)
3	RD+ (Réception de données, signal différentiel positif)
4	Inutilisé
5	Inutilisé
6	RD- (Réception de données, signal différentiel négatif)
7	Inutilisé
8	Inutilisé

illustre la configuration de broches d'une connexion 10BASE-T. La paire qui transmet des données sur une unité est connectée à celle qui reçoit des données sur l'autre unité.

Le choix du mode half-duplex ou full duplex dépend de la configuration. La technologie 10BASE-T prend en charge un trafic de 10 Mbits/s en mode half-duplex et de 20 Mbits/s en mode full duplex.

L'activité de média interactive vous aidera à vous familiariser avec les fonctions de la technologie 10BASE-T.

La page suivante décrit le câblage et l'architecture des systèmes 10BASE-T.

Activité de média interactive

Associer: 10BASE-T

À l'issue de cette activité, les étudiants connaîtront les caractéristiques de la technologie 10BASE-T.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

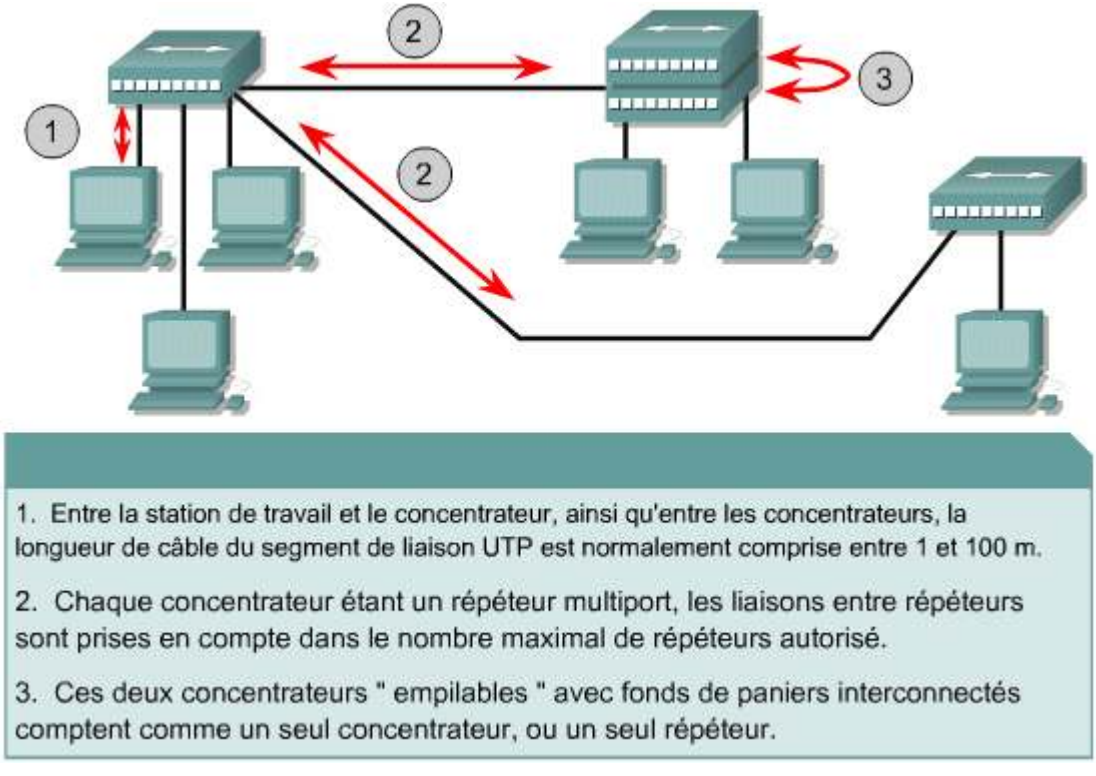
7.1.5 Câblage et architecture des systèmes 10BASE-T

Cette page décrit le câblage et l'architecture des systèmes 10BASE-T.

Une liaison 10BASE-T relie généralement une station à un concentrateur ou à un commutateur. Les concentrateurs sont des répéteurs multiports et sont pris en compte dans la limite des répéteurs entres les stations éloignées. Les concentrateurs ne subdivisent pas les segments de réseau en domaines de collision distincts, contrairement aux ponts et aux commutateurs. La distance maximum entre ponts et commutateurs dépend des restrictions imposées par les médias.

Bien qu'il soit possible d'interconnecter les concentrateurs, il est préférable d'éviter cette configuration. Dans un réseau comportant des concentrateurs interconnectés, le délai d'attente maximum entre deux stations risque d'être dépassé. Lorsque plusieurs concentrateurs sont utilisés, il faut les organiser selon une arborescence hiérarchisée. Pour de meilleures performances, le nombre de répéteurs utilisés entre les stations doit être réduit.

La figure 1


1
2
2
3
1. Entre la station de travail et le concentrateur, ainsi qu'entre les concentrateurs, la longueur de câble du segment de liaison UTP est normalement comprise entre 1 et 100 m.
2. Chaque concentrateur étant un répéteur multiport, les liaisons entre répéteurs sont prises en compte dans le nombre maximal de répéteurs autorisé.
3. Ces deux concentrateurs " empilables " avec fonds de paniers interconnectés comptent comme un seul concentrateur, ou un seul répéteur.

illustre un exemple d'organisation hiérarchisée. La distance séparant une extrémité du réseau à l'autre détermine les limites de l'architecture. Il est essentiel de chercher à réduire au maximum les délais d'attente entre des

stations distantes, quels que soient l'architecture et les types de médias. Plus le délai d'attente maximum sera court, meilleures seront les performances du système.

La longueur sans répéteur des liaisons 10BASE-T peut atteindre 100 m. Bien que cela puisse paraître long, cette distance est courante dans le cadre du câblage d'un bâtiment. Les concentrateurs peuvent résoudre le problème de la distance, mais ils autoriseront la propagation des collisions. Avec l'adoption généralisée des commutateurs, les restrictions de distance sont devenues moins importantes. Si les stations de travail sont situées à 100 m d'un commutateur, la mesure de la distance commence au commutateur.

La page suivante présente la technologie Fast Ethernet.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.6 Ethernet 100 Mbits/s

Cette page présente la technologie Ethernet 100 Mbits/s, également appelée Fast Ethernet. Deux normes sont devenues importantes: 100BASE-TX (câble UTP en cuivre) et 100BASE-FX (fibre optique multimode).

Leurs caractéristiques communes sont les paramètres de synchronisation, le format de trame et certaines parties du processus de transmission. Les technologies 100BASE-TX et 100BASE-FX présentent les mêmes paramètres de synchronisation. Vous remarquerez que la durée d'un bit à 100 Mbits/s = 10 ns = 0,01 microseconde = un cent millionième de seconde. 1

Paramètre	Valeur
Durée d'un bit	10 nanosecondes (ns)
Durée d'une tranche	Durée de 512 bits (64 octets)
Espacement intertrame	96 bits
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)

Le format de trame à 100 Mbits est le même que celui de la trame à 10 Mbits. 2

Trame Ethernet						
Préambule	SFD	Destination	Source	Type de longueur	Données:Bourrage	FCS
7	1	6	6	2	De 46 à 1 500	4

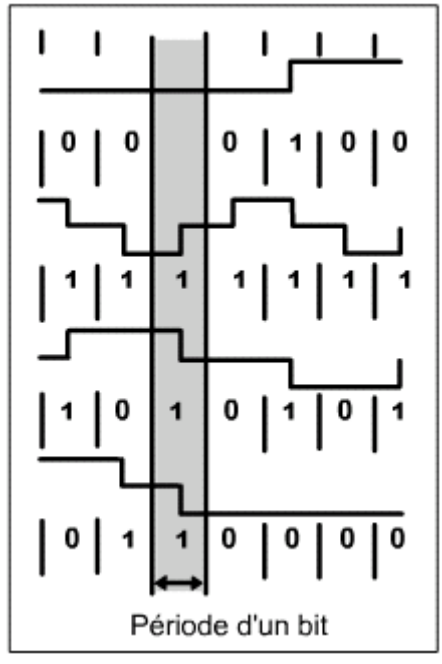
La technologie Fast Ethernet est dix fois plus rapide que la technologie 10BASE-T. Les bits envoyés ont une durée plus courte et leur fréquence est plus élevée. Ces signaux risquent donc plus de générer du bruit. Pour pallier ces problèmes, deux étapes de codage distinctes sont utilisées par les systèmes Ethernet 100 Mbits/s. La première partie du codage emploie une technique appelée «4B/5B», et la deuxième correspond au codage de ligne réel propre au câble en cuivre ou à fibre optique.

La page suivante traite de la norme 100BASE-TX.

Cette page présente la norme 100BASE-TX.

En 1995, le système 100BASE-TX constituait la norme et utilisait les câbles UTP de catégorie 5. Il a connu un véritable essor commercial.

La technologie Ethernet coaxiale d'origine utilisait une transmission en mode half-duplex. De ce fait, une seule unité à la fois pouvait effectuer une transmission. En 1997, la technologie Ethernet a été étendue pour inclure une fonctionnalité full duplex qui permettait à plusieurs ordinateurs d'un réseau de transmettre des données simultanément. Les commutateurs ont remplacé les concentrateurs dans de nombreux réseaux. Ils disposaient en effet de fonctionnalités full duplex et pouvaient rapidement prendre en charge les trames Ethernet.



La technologie 100BASE-TX utilise le codage 4B/5B, qui est ensuite mélangé et converti en codage MLT-3 (*Multi-Level Transmit*). La figure 1

présente quatre ondes différentes. L'onde de la partie supérieure ne comporte aucune transition au centre de la fenêtre de synchronisation. L'absence de transition correspond à un zéro binaire. La deuxième onde comporte une transition au centre de la fenêtre de synchronisation. Cela indique un 1 binaire. La troisième onde présente une séquence binaire en alternance. La quatrième onde permet de constater que le changement de signal correspond aux 1 et les lignes horizontales aux 0.

La figure 2

Nombre de broches	Signal
1	TD+ (Envoi de données, signal différentiel positif)
2	TD- (Envoi de données, signal différentiel négatif)
3	RD+ (Réception de données, signal différentiel positif)
4	Inutilisé
5	Inutilisé
6	RD- (Réception de données, signal différentiel négatif)
7	Inutilisé
8	Inutilisé

illustre la configuration de broches d'une connexion 100BASE-TX. Vous remarquerez la présence des deux chemins de réception-transmission distincts. Cette configuration est identique à celle des systèmes 10BASE-T.

La technologie 100BASE-TX prend en charge le trafic 100 Mbits/s en mode half-duplex. Avec ce mode, les systèmes 100BASE-TX peuvent échanger des données à un débit de 200 Mbits/s. Le mode full duplex va prendre de plus en plus d'importance au fur et à mesure que de l'augmentation de la vitesse de la technologie Ethernet.

La page suivante présente les câbles à fibre optique de Fast Ethernet.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

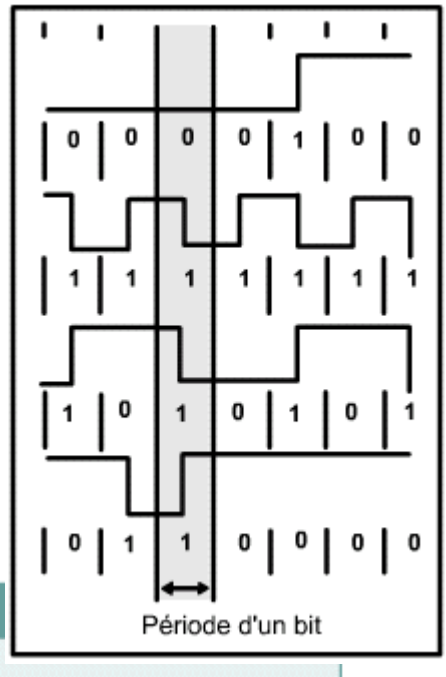
7.1.8 100BASE-FX

Cette page présente la technologie 100BASE-FX.

Lors de l'introduction de la technologie Fast Ethernet avec un câblage en cuivre, le besoin d'une version à fibre optique était également ressenti. La fibre optique pouvait en effet être utilisée pour les applications de backbone, pour les connexions entre étages, dans les bâtiments où le cuivre était peu souhaitable, ainsi que dans les environnements où le bruit est important. La technologie 100BASE-FX a donc été employée pour répondre à cette demande. Toutefois, cela n'a jamais été une réelle réussite. En effet, les normes Gigabits Ethernet à câbles en cuivre et à fibre optique ont ensuite été introduites. Ces normes sont désormais préférées pour les installations en backbone, les interconnexions à haut débit et l'infrastructure en général.

La temporisation, le format de trame et le mode de transmission sont identiques pour les versions cuivre et fibre optique de Fast Ethernet 100 Mbits/s. Cependant, 100BASE-FX utilise l'encodage NRZI, qui est montré dans la figure 1.

La partie supérieure de la courbe ne présente pas de transition, ce qui indique une valeur binaire nulle. Dans la deuxième onde, la transition au centre de la fenêtre de synchronisation indique un 1 binaire. La troisième onde présente une séquence binaire en alternance. Dans les troisième et quatrième ondes, il apparaît plus clairement que l'absence de transition correspond à un 0 binaire et que la présence d'une transition indique un 1 binaire.



La figure 2

Fibre	Signal
1	Tx (LED et émetteurs laser)
2	Rx (détecteurs photodiodes à haut débit)

illustre une configuration de broches et une liaison 100BASE-FX. Une paire en fibre optique associée à des connecteurs ST ou SC est le plus souvent utilisée.

Les chemins de transmission (TX) et de réception (Rx) de la technologie 100BASE-FX à fibre optique permettent chacun des transmissions à 200 Mbits/s.

La page suivante décrit l'architecture Fast Ethernet.

7.1 Ethernet 10 Mbits/s et 100 Mbits/s

7.1.9 Architecture Fast Ethernet

Cette page décrit l'architecture de la technologie Fast Ethernet.

Les liaisons Fast Ethernet se composent généralement d'une connexion entre une station et un concentrateur ou un commutateur. Les concentrateurs sont des répéteurs multiports et les commutateurs correspondent à des ponts multiports. Ils sont soumis aux restrictions de distance des médias UTP, à savoir 100 m.

Un répéteur de classe I peut introduire une latence d'une durée allant jusqu'à 140 bits. Tout répéteur modifié entre une implémentation Ethernet et une autre appartient à la classe I. Les délais de synchronisation d'un répéteur de classe II sont plus courts (durée de 92 bits), car ce type de matériel répète immédiatement le signal entrant vers tous les autres ports, sans processus de conversion. Pour pouvoir offrir un tel délai, les répéteurs de classe II peuvent uniquement se connecter à des types de segments qui utilisent la même technique de signalisation.

À l'instar des versions à 10 Mbits/s, les version à 100 Mbits/s autorisent la modification de certaines règles d'architecture. Cela est cependant fortement déconseillé pour les systèmes 100BASE-TX. La longueur de câble 100BASE-TX entre les répéteurs de classe II ne doit pas être supérieure à 5 m. Il n'est pas rare de rencontrer des liaisons qui fonctionnent en mode half-duplex dans les systèmes Fast Ethernet. Toutefois, ce mode est déconseillé car le schéma de signalisation est en mode full duplex.

La figure 1

Architecture	100BASE-TX	100BASE-FX	100BASE-TX et FX
De station à station, de station à commutateur, de commutateur à commutateur (half ou full duplex)	100 m	412 m	N/A
Un répéteur de classe I (half-duplex)	200 m	272 m	100 m (TX) 160.8 m (FX)
Un répéteur de classe II (half-duplex)	200 m	320 m	100 m (TX) 208 m (FX)
Deux répéteurs de classe II (half-duplex)	205 m	228 m	105 m (TX) 211.2 m (FX)

illustre les longueurs de câbles nécessaires pour l'architecture. La longueur maximale sans répéteur des liaisons 100BASE-TX peut atteindre 100 m. Avec les commutateurs, cette restriction est devenue moins importante. La plupart des réseaux Fast Ethernet sont commutés.

Cette page termine la leçon. La leçon suivante présente la technologie Gigabit Ethernet et 10 Gigabit Ethernet. La première page décrit les normes Ethernet 1 000 Mbits/s.

Activité de TP

Exercice: Introduction à Fluke Network Inspector

Ce TP explique comment utiliser le programme Fluke Networks Network Inspector (NI) pour détecter et analyser les équipements réseau dans un domaine de broadcast.

Activité de TP

Exercice: Introduction à Fluke Protocol Inspector

Ce TP explique comment utiliser Fluke Networks Protocol Inspector pour analyser le trafic réseau et les trames de données.

Activité de média interactive

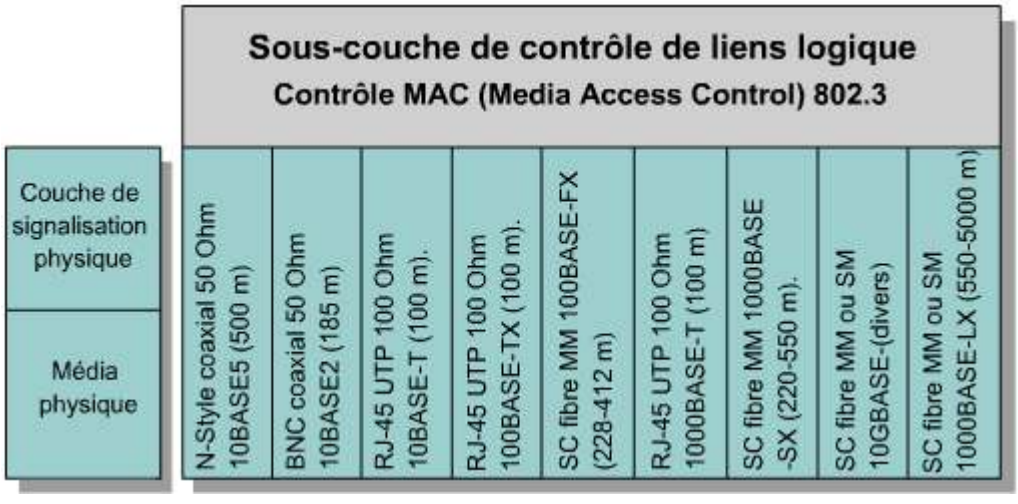
Glisser-Positionner: Architecture Fast Ethernet

À l'issue de cette activité, les étudiants comprendront l'architecture Fast Ethernet.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.1 Ethernet 1 000 Mbits/s

Cette page décrit les normes Ethernet 1 000 Mbits/s ou Gigabit. Ces normes peuvent utiliser des médias à fibre optique ou en cuivre pour la transmission des données. 1


Sous-couche de contrôle de liens logique
Contrôle MAC (Media Access Control) 802.3
Couche de signalisation physique
Média physique
N-Style coaxial 50 Ohm 10BASE5 (500 m)
BNC coaxial 50 Ohm 10BASE2 (185 m)
RJ-45 UTP 100 Ohm 10BASE-T (100 m).
RJ-45 UTP 100 Ohm 100BASE-TX (100 m).
SC fibre MM 100BASE-FX (228-412 m)
RJ-45 UTP 100 Ohm 1000BASE-T (100 m)
SC fibre MM 1000BASE -SX (220-550 m).
SC fibre MM ou SM 10GBASE-(divers)
SC fibre MM ou SM 1000BASE-LX (550-5000 m)

La norme 1000BASE-T (IEEE 802.3ab) utilise un câblage en cuivre équilibré de catégorie 5 ou supérieure. La norme 1000BASE-X (IEEE 802.3z) définit un débit de 1 Gbit/s en mode full duplex, avec fibre optique.

Les normes 1000BASE-TX, 1000BASE-SX et 1000BASE-LX utilisent les mêmes paramètres de synchronisation, comme l'illustre la figure 2

Paramètre	Valeur
Types Ethernet	1 ns
Durée d'une tranche	Durée de 4 096 bits
Espacement intertrame	96 bits *
Nombre maximum de tentatives après collision	16
Nombre maximum de réémissions temporisées après collision	10
Taille du signal de collision	32 bits
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)
Limite de débit garanti en rafale	65 536 bits

* La valeur indiquée correspond à l'espacement officiel intertrame.

.

La durée d'un bit est de 1 ns, 0,000000001 seconde ou 1 milliardième de seconde. La trame Gigabit Ethernet présente le même format que celle d'Ethernet 10 Mbits/s et 100 Mbits/s. Certaines mises en œuvre de la technologie Gigabit Ethernet peuvent utiliser différents processus pour convertir des trames en bits sur le câble. La figure 3

Trame Ethernet						
Préambule	SFD	Destination	Source	Type de longueur	Données Bourrage	FCS
7	1	6	6	2	De 46 à 1 500	4

illustre les champs de trame Ethernet.

Les différences entre les normes Ethernet, Fast Ethernet et Gigabit Ethernet apparaissent au niveau de la couche physique. En raison de la vitesse accrue de ces nouvelles normes, la réduction de la durée de bit implique des considérations spéciales. Les bits étant introduits plus fréquemment sur le support pour une durée plus courte, la synchronisation est très importante. La transmission à haut débit nécessite une fréquence plus élevée. Cela résulte en une plus grande vulnérabilité des bits au bruit sur des médias en cuivre.

La norme Gigabit Ethernet doit donc utiliser deux étapes de codage distinctes. La transmission des données est plus efficace lorsque les codes sont utilisés pour représenter le train binaire. Le codage des données permet la synchronisation, l'utilisation efficace de la bande passante. Cela améliore également le rapport signal/bruit.

Au niveau de la couche physique, le profil binaire de la couche MAC est converti en symboles. Ces symboles peuvent aussi représenter des informations de contrôle, telles que le début de trame, la fin de trame ou les conditions d'inactivité sur une liaison. La trame est codée sous forme de symboles de contrôle et de symboles de données pour augmenter le débit sur le réseau.

La norme Gigabit Ethernet à fibre optique (1000BASE-X) utilise le codage 8B/10B, qui est semblable au concept 4B/5B. Il est suivi par le codage de ligne simple de non-retour à zéro (NRZ) de la lumière sur les fibres optiques. Ce processus de codage est possible car le support à fibre optique peut prendre en charge des signaux de bande passante plus large.

La page suivante traite de la norme 1000BASE-T.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.2 1000BASE-T

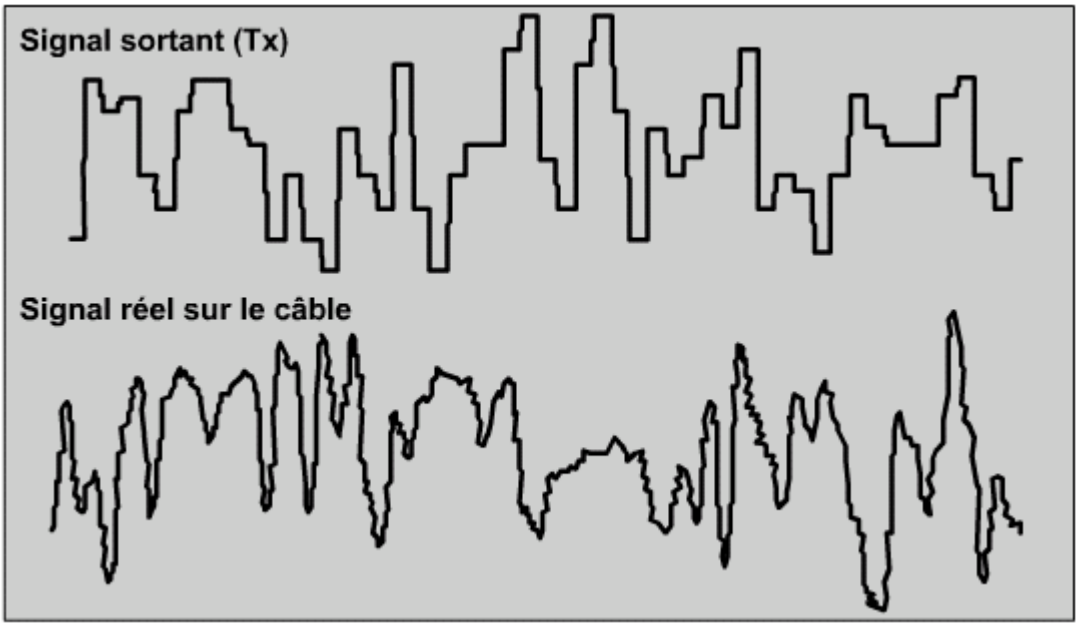
Cette page décrit la norme 1000BASE-T.

Lorsque la norme Fast Ethernet a été installée pour augmenter la bande passante des stations de travail, des goulots d'étranglement sont apparus en amont du réseau. La norme 1000BASE-T (IEEE 802.3ab) a été développée pour fournir une bande passante supplémentaire afin de désengorger ces goulots d'étranglement. Cela a permis un débit plus important pour les unités telles que les backbones entre les bâtiments, les liaisons entre les commutateurs, les fermes de serveurs ou d'autres applications de locaux techniques. Cela a également fournit des connexions pour les stations de travail haut de gamme. Fast Ethernet a été conçu pour fonctionner avec un câble en cuivre de catégorie 5 ayant réussi le test de la catégorie 5e. La plupart des câbles de catégorie 5 installés peuvent obtenir la certification de catégorie 5e si leur connexion est adaptée. Il est important que la norme 1000BASE-T soit compatible avec les normes 10BaseT et 100BaseTX.

Étant donné qu'un câble 5e peut supporter sans risque un débit maximal de 125 Mbits/s, une bande passante de 1 000 Mbits/s ou d'un gigabit était un véritable défi. La première étape de la mise en œuvre de la norme 1000BASE-T consiste à utiliser les quatre paires de fils plutôt que les deux paires généralement utilisées par les normes 10BASE-T et 100BASE-TX. Cela nécessite un circuit complexe qui permet d'effectuer des transmissions en mode full duplex sur la même paire de fils. Ainsi, chaque paire dispose d'un débit de 250 Mbits/s. Ainsi, avec les quatre paires de fils, il est possible d'obtenir les 1 000 Mbits/s souhaités. Les informations étant transmises simultanément sur les quatre chemins, le circuit doit diviser les trames au niveau de l'émetteur et les réunir au niveau du récepteur.

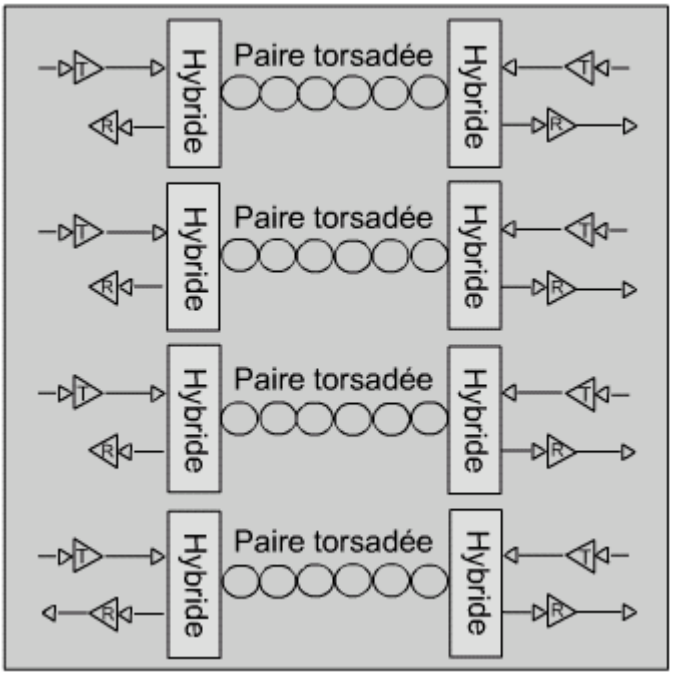
Le codage 1000BASE-T avec le codage de ligne 4D-PAM5 est utilisé sur un câble de catégorie 5e, ou encore mieux, sur un câble UTP. Cela signifie que la transmission et la réception des données sont effectuées dans les deux sens sur le même fil et simultanément. Cela entraîne par conséquent une collision permanente sur les paires de fils. Ces collisions sont à l'origine de profils électriques complexes. Avec des circuits intégrés complexes qui utilisent des techniques telles que l'annulation de l'écho, la correction des erreurs de la couche 1 ou la sélection prudente des niveaux de tension, le système peut proposer un débit de 1 gigabit.

Pendant les périodes d'inactivité, il existe neuf niveaux de tension sur le câble, contre 17 lors de la transmission des données. 1



Avec ce nombre important d'états et les effets de bruit, le signal semble plus analogique que numérique. À l'instar des signaux analogiques, le système risque plus de générer du bruit en raison du câble et des problèmes de raccordement.

Les données de la station expéditrice sont soigneusement réparties en quatre courants parallèles, puis codées, transmises et détectées en parallèle. Enfin, elles sont de nouveau assemblées en un train binaire de réception. La figure 2



représente le mode full duplex simultané sur quatre paires de fils. La norme 1000BASE-T prend en charge les actions en mode half-duplex et full duplex. L'utilisation de cette norme en mode full duplex est très répandue.

La page suivante présente les normes 1000BASE-SX et LX.

7.2 Gigabit et 10 Gigabit Ethernet
7.2.3 1000BASE-SX et LX

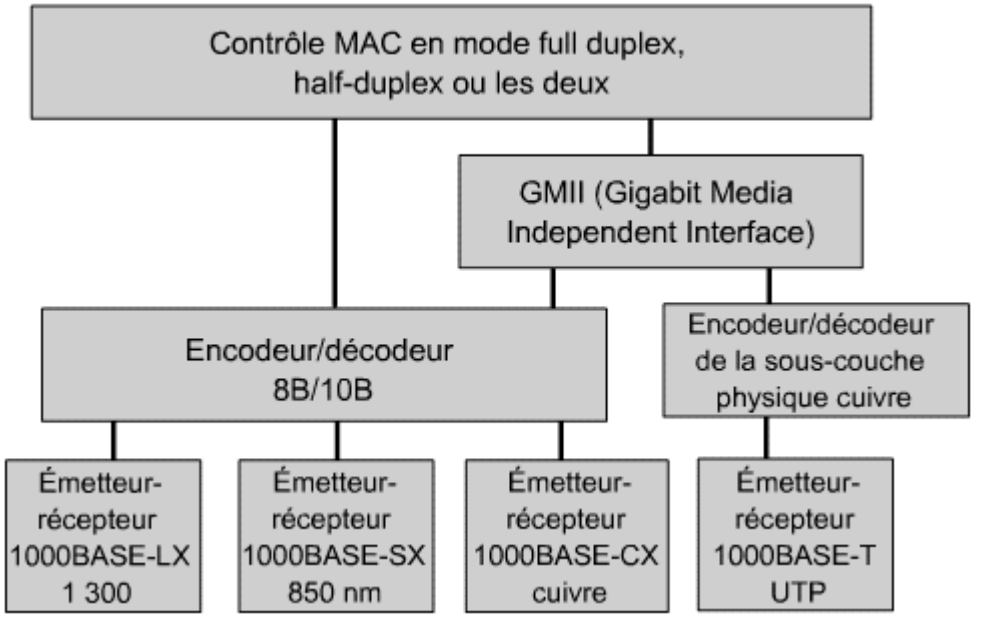
Cette page décrit les systèmes à fibre optique monomodes et multimodes.

La norme IEEE 802.3 recommande d'utiliser la norme Gigabit Ethernet sur des fibres optiques pour le backbone. 1

Avantages de Gigabit Ethernet sur fibre optique

- Absence de bruit
- Pas de risques de problèmes de mise à la terre
- Excellentes caractéristiques de longueur
- De nombreuses options 1000BASEX
- Peut être utilisé pour connecter des sections Fast Ethernet dispersées sur une grande échelle.

La synchronisation, le format de trame et la transmission sont communs à toutes les versions à 1 000 Mbits/s. Deux systèmes de codage des signaux sont définis au niveau physique. 2


Contrôle MAC en mode full duplex, half-duplex ou les deux
GMII (Gigabit Media Independent Interface)
Encodeur/décodeur 8B/10B
Encodeur/décodeur de la sous-couche physique cuivre
Émetteur-récepteur 1000BASE-LX 1 300
Émetteur-récepteur 1000BASE-SX 850 nm
Émetteur-récepteur 1000BASE-CX cuivre
Émetteur-récepteur 1000BASE-T UTP

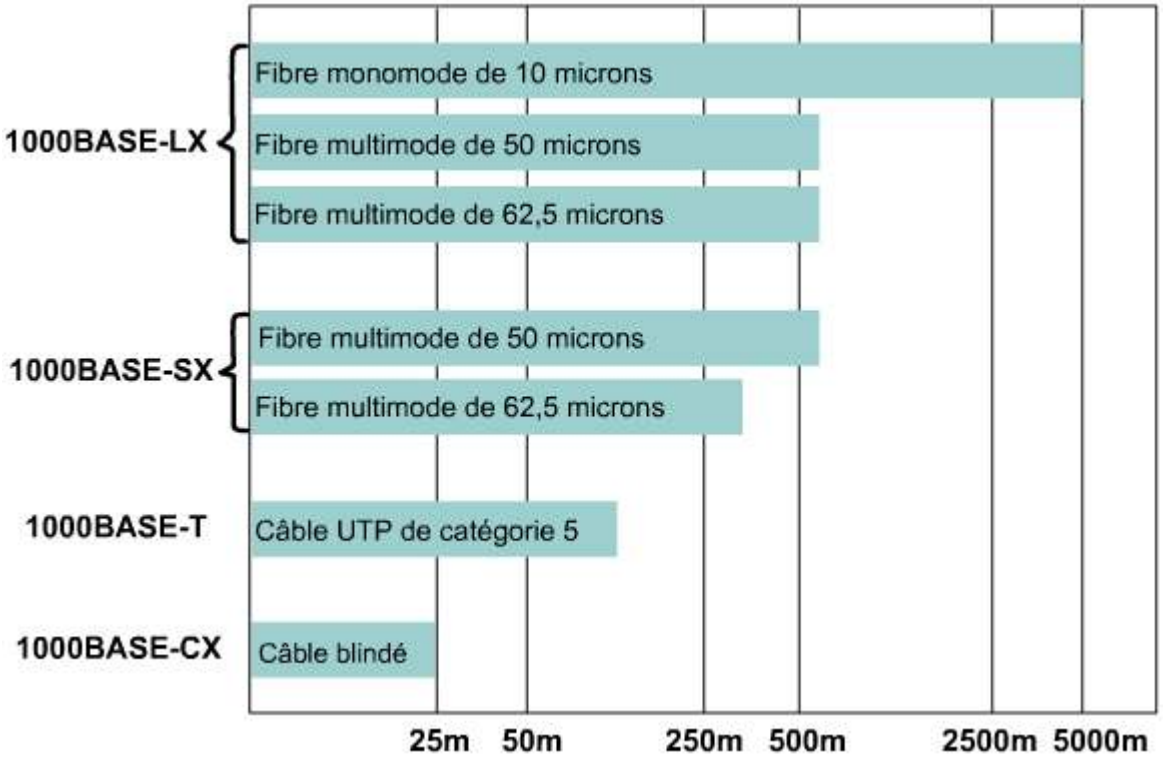
Le système 8B/10B est utilisé pour les médias à fibre optique et en cuivre blindés, tandis que la modulation d'impulsions en amplitude PAM5 (*pulse amplitude modulation 5*) l'est pour les câbles UTP.

La norme 1000BASE-X fait appel au codage 8B/10B converti en codage de ligne de non-retour à zéro (NRZ). Le codage NRZ utilise le niveau de signal de la fenêtre de synchronisation pour déterminer la valeur binaire de cette période de bits. Contrairement à la plupart des autres systèmes de codage décrits, celui-ci est fonction du niveau, et non de la limite définie . Cela signifie que pour déterminer si un bit correspond à un 0 ou à un 1, le système se réfère au niveau du signal plutôt qu'au moment où le signal change de niveau.

Les signaux NRZ sont ensuite transmis à la fibre sous forme d'impulsions en utilisant des sources lumineuses à ondes longues ou courtes. Les ondes courtes sont fournies par un laser de 850 nm ou une source LED sur des

fibres optiques multimodes (1000BASE-SX). Cette option est la moins onéreuse, mais les distances autorisées sont plus courtes. La source laser de 1 310 nm des ondes longues utilise des fibres optiques (1000BASE-LX) monomodes ou multimodes. La longueur des fibres optiques monomodes employées peut atteindre 5 000 mètres. En raison de la durée requise à chaque fois pour mettre totalement sous tension ou hors tension la LED ou le laser, la lumière est émise sous forme d'impulsions à basse ou haute tension. Un 0 logique est représenté par une basse tension, et un 1 logique par une haute tension.

La méthode MAC (*Media Access Control*) traite la liaison comme étant de type point-à-point. Différentes fibres optiques étant utilisées pour la transmission (Tx) et la réception (Rx), la connexion est, de façon inhérente, en mode full duplex. La norme Gigabit Ethernet n'autorise qu'un seul répéteur entre deux stations. La figure 3



représente un tableau de comparaison des médias Ethernet 1000BASE.

La page suivante décrit l'architecture de la technologie Gigabit Ethernet.

Activité de média interactive

Glisser-Positionner: Comparaison entre les différents médias Gigabit Ethernet

À l'issue de cette activité, les étudiants seront capables de faire la distinction entre les médias Gigabit Ethernet.

Activité de média interactive

Case à cocher: Versions «fibre» de Gigabit Ethernet

À l'issue de cette activité, les étudiants seront capables d'identifier la norme Gigabit Ethernet à fibre optique.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.4 Architecture Gigabit Ethernet

Cette page décrit l'architecture de la norme Gigabit Ethernet.

La longueur des liaisons en mode full duplex est uniquement limitée par le support, et non par le temps de parcours aller-retour entre deux hôtes. La plupart des réseaux Gigabit Ethernet étant commutés, les valeurs des figures 1 et 2

Média	Bande passante modale	Longueur maximale
Fibre multimode 62,5 µm	160	220 m
Fibre multimode 62,5 µm	200	275 m
Fibre multimode 50 µm	400	500 m
Fibre multimode 50 µm	500	500 m

Média	Bande passante modale	Longueur maximale
Fibre multimode 62,5 µm	500	550 m
Fibre multimode 50 µm	400	550 m
Fibre multimode 50 µm	500	550 m
Fibre multimode 10 µm	N/A	5000 m

correspondent aux limites pratiques entre les unités. Les topologies en étoile, en étoile étendue et chaînée sont toutes autorisées. Les points importants sont alors la topologie logique et le flux de données, non la synchronisation ou les restrictions de distance.

Un câble UTP 1000BASE-T est identique à un câble 10BASE-T ou 100BASE-TX, mais la performance des liaisons doit satisfaire aux exigences de qualité supérieure de la catégorie 5e ou de la classe D ISO (2000).

Il est fortement déconseillé de modifier les règles d'architecture de la norme 1000BASE-T. Avec une distance de 100 mètres, le matériel fonctionne à la limite de ses capacités pour récupérer le signal transmis. Tout problème de câblage ou bruit peut empêcher le fonctionnement d'un câble conforme, même si la distance entre dans les limites spécifiées.

Il est conseillé d'autoriser l'autonégociation pour toutes les liaisons entre une station et un concentrateur ou un commutateur pour bénéficier des meilleures performances communes. Cela évitera des problèmes liés à une configuration incorrecte des autres paramètres requis pour une bonne utilisation de Gigabit Ethernet.

La page suivante présente la norme 10 Gigabit Ethernet.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.5 10 Gigabit Ethernet

Cette page décrit la norme 10 Gigabit Ethernet et la compare à d'autres versions d'Ethernet.

La norme IEEE 802.3ae a été adaptée pour inclure la transmission en mode full duplex de 10 Gbits/s sur un câblage à fibre optique. Les similitudes de base entre les normes 802.3ae et 802.3, système Ethernet d'origine,

peuvent être facilement constatées. Cette norme 10 Gigabit Ethernet (10GbE) est évolutive non seulement pour les LAN, mais aussi pour les MAN et WAN.

Avec un format de trame et d'autres spécifications de couche 2 d'Ethernet conformes aux normes précédentes, 10 Gigabit Ethernet peut fournir une bande passante plus large utilisable avec l'infrastructure réseau existante.

Une évolution de concept importante pour Ethernet apparaît cependant avec cette nouvelle norme. Les systèmes Ethernet sont généralement assimilés à une technologie LAN, mais les spécifications de la couche physique 10 Gigabit Ethernet permettent d'étendre les distances jusqu'à 40 km sur une fibre optique monomode tout en assurant la compatibilité avec un réseau optique synchrone (SONET) et des réseaux à hiérarchie numérique synchrone (SDH). Grâce à cette plus grande flexibilité au niveau des distances, 10 Gigabit Ethernet peut être classée comme une technologie MAN exploitable. Qui plus est, sa compatibilité avec les réseaux SONET et SDH [qui atteignent le niveau de vitesse OC-192 (9,584640 Gbits/s)] en fait une technologie WAN valide. Pour certaines applications, cette norme peut également entrer en concurrence avec la technologie ATM.

Récapitulons les points communs et les différences entre la norme 10 Gigabit Ethernet et les autres versions de la technologie Ethernet: 1

Paramètre	Valeur
Durée d'un bit	0,1 ns
Durée d'une tranche	Non applicable *
Espacement intertrame	96 bits **
Nombre maximum de tentatives après collision	Non applicable *
Nombre maximum de réémissions temporisées après collision	Non applicable *
Taille du signal de collision	Non applicable *
Taille maximale des trames non référencées	1 518 octets
Taille minimale des trames	512 bits (64 octets)
Limite de débit garanti en rafale	Non applicable *
Taux d'extension de l'espacement intertrame	104 bits ***

* 10 Gigabit Ethernet ne permettant pas un fonctionnement en mode half-duplex, les paramètres associés à la durée d'une tranche et à la gestion des collisions ne sont pas applicables.
** La valeur indiquée correspond à l'espacement officiel intertrame.

- Le format de trame est identique, offrant ainsi une interopérabilité entre toutes les versions initiales, Fast, Gigabit et 10 Gigabit, sans redéfinir la trame ni convertir les protocoles.
- La durée d'un bit est désormais de 0,1 nanoseconde. Toutes les autres variables de temps s'adaptent en conséquence.
- Étant donné que seules les connexions à fibre optique en mode full duplex sont utilisées, CSMA/CD n'est pas requis.
- Les sous-couches IEEE 802.3 des couches 1 et 2 OSI sont pour la plupart préservées, avec quelques ajouts pour permettre les liaisons à fibre optique sur 40 km et l'interopérabilité avec les réseaux SONET et SDH.
- Il est désormais possible de disposer de réseaux Ethernet de bout en bout flexibles, efficaces, fiables et relativement peu onéreux.
- Le protocole TCP/IP peut être utilisé sur des réseaux LAN, MAN et WAN avec une méthode de transport de couche 2.

La norme de base IEEE 802.3 prend en charge la méthode CSMA/CD. Un complément de cette norme (802.3ae) décrit la technologie 10 Gigabit Ethernet. Comme cela est souvent le cas pour les nouvelles technologies, plusieurs implémentations sont prises en compte:

- **10GBASE-SR:** conçue pour les courtes distances sur des fibres optiques multimodes déjà installées, supporte une distance de 26 à 82 m.
- **10GBASE-LX4:** utilise le multiplexage de longueurs d'onde, supporte une distance de 240 à 300 m sur des fibres optiques multimodes déjà installées et 10 km sur des fibres optiques monomodes.
- **10GBASE-LR et 10GBASE-ER:** supportent une distance de 10 km et 40 km respectivement sur des fibres optiques monomodes.
- **10GBASE-SW, 10GBASE-LW et 10GBASE-EW:** généralement appelées « 10GBase-W », conçues pour fonctionner avec un équipement de réseaux WAN SONET et SDH, avec module de transport synchrone OC-192.

Le groupe de travail de la norme IEEE 802.3ae et l'alliance 10 Gigabit Ethernet (10GEA) étudient la normalisation de ces technologies émergentes.

La norme 10 Gigabit Ethernet (IEEE 802.3ae) a été élaborée en juin 2002. Il s'agit d'un protocole en mode full duplex qui utilise uniquement la fibre optique comme support de transmission. La distance maximale de transmission dépend du type de fibre utilisé. Avec les fibres monomodes, cette distance est de 40 km. Au fur et à mesure des discussions entre les membres IEEE, on commence à envisager la possibilité d'une création de normes pour les technologies 40, 80 et même 100 Gigabit Ethernet.

La page suivante présente l'architecture de la norme 10 Gigabit Ethernet.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.6 Architectures 10 Gigabit Ethernet

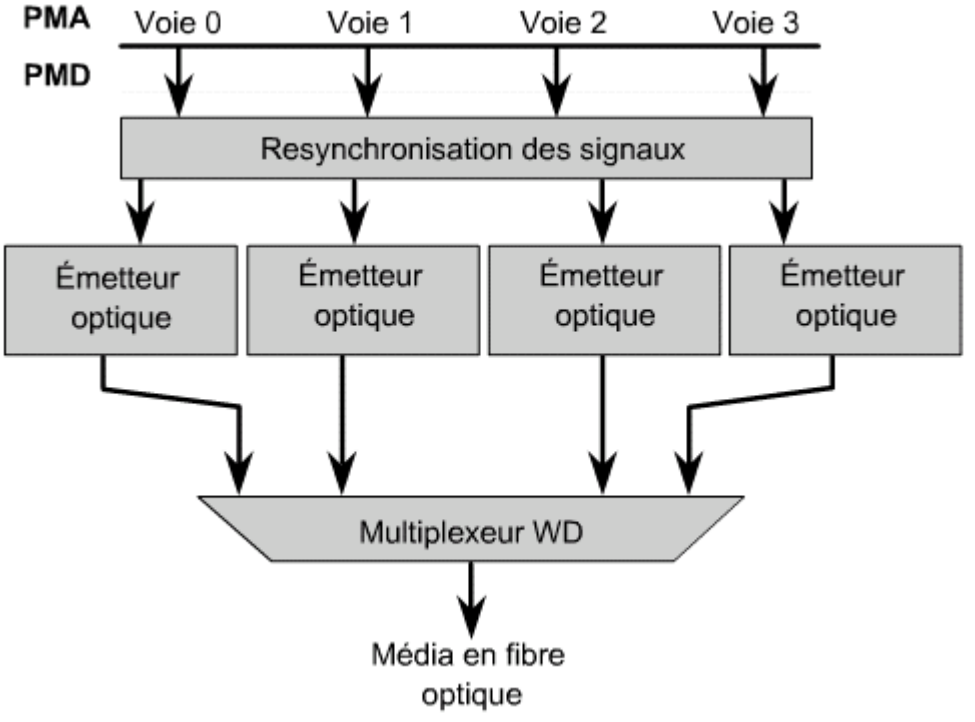
Cette page décrit les architectures 10 Gigabit Ethernet.

Comme cela a été le cas lors du développement de la technologie Gigabit Ethernet, l'augmentation de la vitesse entraîne de nouvelles exigences. La durée de bit plus courte qui résulte de l'augmentation de la vitesse oblige à prendre en compte un certain nombre de considérations particulières. Pour les transmissions 10 Gigabit Ethernet, chaque bit de données dure 0,1 nanoseconde. Cela signifie que 1 000 bits de données Gigabit Ethernet sont transmis pour une même durée de bit qu'un bit de données d'un flux de données Ethernet 10 Mbits/s. En raison de la courte durée du bit de données 10 Gigabit Ethernet, il est souvent difficile de séparer un bit de données du bruit. Les transmissions de données 10 Gigabit Ethernet nécessitent une synchronisation de bits exacte afin que les données soient distinguées des effets de bruit sur la couche physique. C'est là l'objet de la synchronisation.

Pour traiter ces questions de synchronisation, de bande passante et de rapport signal/bruit, les systèmes 10 Gigabit Ethernet font appel à deux étapes de codage distinctes. L'utilisation de codes pour représenter les données utilisateur rend la transmission plus efficace. Ce codage permet la synchronisation, l'utilisation efficace de la bande passante. Cela améliore également le rapport signal/bruit.

Des trains binaires en série complexes sont utilisés dans toutes les versions de la norme 10 Gigabit Ethernet, à l'exception de 10GBASE-LX4, qui repose sur la technologie WWDM (*Wide Wavelength Division Multiplex*) pour procéder au multiplexage des quatre trains binaires simultanés lorsque quatre ondes sont propagées simultanément dans la fibre.

La figure 1



illustre le cas particulier de l'utilisation de quatre sources laser, dont les longueurs d'onde sont légèrement différentes. Lorsque le flux du signal optique atteint le support, il est démultiplexé en quatre flux de signaux optiques distincts. Ces flux sont ensuite convertis en quatre trains de bits électroniques lorsqu'ils effectuent pratiquement le chemin inverse via les sous-couches de la couche MAC.

Actuellement, la plupart des produits 10 Gigabits Ethernet existent sous forme de modules, ou de cartes d'interface, qui sont ajoutés aux commutateurs et aux routeurs haut de gamme. Au fil de l'évolution des technologies 10 Gigabit Ethernet, la diversité des composants de signalisation sera plus grande. De même, tout au long de l'évolution des technologies optiques, des émetteurs et des récepteurs améliorés vont être intégrés à ces produits, qui bénéficieront davantage de la modularité. Toutes les versions de la norme 10 Gigabit Ethernet reposent sur l'utilisation de médias à fibre optique. Les types de fibre sont les fibres monomodes de 10 µ et les fibres multimodes de 50 et 62,5 µ. Plusieurs caractéristiques de dispersion et d'atténuation des fibres sont prises en charge, mais les distances d'utilisation sont limitées.

Bien que cette prise en charge ne concerne que le média à fibre optique, certaines longueurs de câble maximales sont étonnamment courtes. 2

Mise en œuvre	Longueur d'	Média	Bande passante modale minimale	Longueur d'exploita
10GBASE-LX4	1310 nm	62.5µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	50µm MMF	400 MHz/km	2 - 240 m
10GBASE-LX4	1310 nm	50µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	10µm MMF	N/A	2 - 10 km
10GBASE-S	850 nm	62.5µm MMF	160 MHz/km	2 - 26 m
10GBASE-S	850 nm	62.5µm MMF	200 MHz/km	2 - 33 m
10GBASE-S	850 nm	50µm MMF	400 MHz/km	2 - 66 m
10GBASE-S	850 nm	50µm MMF	500 MHz/km	2 - 82 m
10GBASE-S	850 nm	50µm MMF	2000 MHz/km	2 - 300 m
10GBASE-L	1310 nm	10µm SMF	N/A	2 - 10 km
10GBASE-E	1550 nm	10µm SMF	N/A	2 - 30 km

Aucun répéteur n'est défini pour la norme 10 Gigabit Ethernet, le mode half-duplex n'étant explicitement pas pris en charge.

Comme pour les versions à 10, 100 et 1 000 Mbits/s, il est possible de légèrement modifier certaines règles d'architecture. Ces ajustements autorisés sont liés à la perte de signal et à la distorsion qui surviennent sur le support. À cause de la dispersion du signal et d'autres problèmes, il devient impossible de lire l'impulsion lumineuse au-delà de certaines distances.

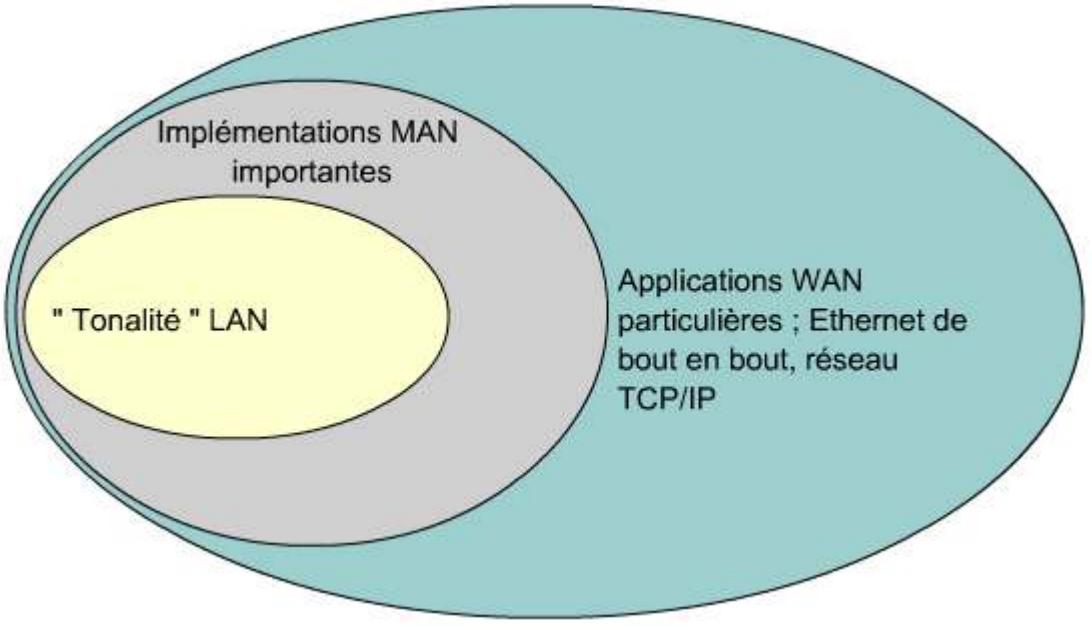
La page suivante traite de l'avenir d'Ethernet.

7.2 Gigabit et 10 Gigabit Ethernet

7.2.7 Avenir d'Ethernet

Cette page explique aux étudiants quel est l'avenir d'Ethernet.

La technologie Ethernet a connu l'évolution suivante: version initiale —> Fast —> Gigabit —> MultiGigabit. Alors que d'autres technologies LAN sont toujours utilisées (installations existantes), la norme Ethernet est largement employée dans les nouvelles installations LAN; à tel point que certains ont qualifié Ethernet de «tonalité» LAN. Ethernet est désormais la norme pour les connexions horizontales, verticales et entre les bâtiments. Les dernières versions d'Ethernet en cours de développement sont en train d'atténuer les différences existant entre les réseaux LAN, MAN et WAN. 1



Alors que la norme 1 Gigabit Ethernet est désormais largement commercialisée et que les produits 10 Gigabit deviennent plus disponibles, l'IEEE et l'alliance 10 Gigabit Ethernet travaillent sur les normes 40, 100 et même 160 Gbits/s. Les technologies adoptées vont dépendre de plusieurs facteurs, notamment du niveau de maturation des technologies et des normes, ou encore du taux d'implantation sur les marchés et du coût.

Des propositions pour des modèles d'arbitrage d'Ethernet autres que CSMA/CD ont été émises. Le problème des collisions avec les topologies de bus physique des concentrateurs 10BASE5/10BASE2 et 10BASE-T/100BASE-TX se rencontre de moins en moins fréquemment. L'utilisation de câblages UTP et à fibre optique avec des chemins Tx et Rx distincts, ainsi que la diminution des coûts des commutateurs limitent l'importance des connexions pour médias partagés uniques ou half-duplex.

L'avenir des médias réseau peut se décomposer en trois phases:

- La phase cuivre (jusqu'à 1 000 Mbits/s, voire plus).
- La phase sans fil (approchant les 100 Mbits/s, voire plus).
- La phase fibre optique (actuellement à 10 000 Mbits/s, devrait bientôt dépasser ce seuil).

Les médias en cuivre et sans fil présentent des limites physiques et pratiques au niveau des signaux à haute fréquence émis. Cela ne sera pas le cas pour la fibre optique. Les capacités de la bande passante sur fibre optique sont vastes et aucun problème de restriction ne s'est encore posé. Dans les systèmes à fibre optique, ce sont essentiellement les processus de fabrication des fibres et la technologie électronique (telle que les émetteurs et les détecteurs) qui limitent la vitesse. À l'avenir, l'utilisation de sources lumineuses laser et de la fibre optique monomode prévaudra fortement dans l'évolution d'Ethernet.

À l'époque où Ethernet était plus lent, en mode half-duplex, soumis à des collisions et qu'il constituait un processus «démocratique» de hiérarchisation, ses fonctionnalités relatives à la qualité de service étaient jugées insuffisantes pour traiter certains types de trafic. Il s'agissait alors de la téléphonie IP et du multicast vidéo.

Les technologies Ethernet à haut débit et en mode full duplex qui dominent désormais le marché s'avèrent suffisantes pour prendre en charge les applications exigeantes en termes de qualité de service. L'éventail des applications potentielles d'Ethernet s'en trouve ainsi élargi. Curieusement, parce qu'elle offrait une qualité de service de bout en bout, la technologie ATM s'est trouvée propulsée dans les bureaux et les réseaux WAN au milieu des années 90, mais c'est maintenant Ethernet qui est sur le point de l'emporter.

Cette page termine la leçon. La page suivante récapitule les principaux points évoqués au cours de ce module.

Résumé

Cette page résume les sujets traités dans ce module.

Ethernet est une technologie dont la vitesse a été multipliée par 1 000, de 10 à 10 000 Mbits/s, en moins d'une décennie. Toutes les versions d'Ethernet présentent une structure de trame similaire, permettant une excellente interopérabilité. La plupart des connexions en cuivre Ethernet sont désormais en mode full duplex commuté, et la technologie Ethernet avec câblage en cuivre la plus rapide est 1000BASE-T, ou Gigabit Ethernet. La technologie 10 Gigabit Ethernet et les versions plus rapides utilisent essentiellement des fibres optiques.

Les technologies Ethernet 10BASE5, 10BASE2 et 10BASE-T sont considérées comme les versions initiales d'Ethernet. Elles ont en commun quatre caractéristiques, à savoir les paramètres de synchronisation, le format de la trame, le processus de transmission et la règle de conception de base.

Elles codent les données sur un signal électrique. La forme de codage utilisée dans les systèmes de 10 Mbits/s est appelée « codage Manchester ». Ce type de codage repose sur les changements de tension pour représenter les nombres binaires 0 et 1. Une hausse ou une baisse de la tension pendant une certaine durée (période de bits) détermine la valeur binaire du bit.

Outre une période de bits standard, les normes Ethernet définissent des limites pour les tranches de temps et l'espacement intertrame. La durée des transmissions est fonction du type de média utilisé et des normes de synchronisation garantissent l'interopérabilité. La fenêtre temporelle de la technologie Ethernet de 10 Mbits/s se caractérise par un ensemble pouvant comprendre jusqu'à cinq segments séparés par un maximum de quatre répéteurs.

Le câble coaxial fin unique a été le premier support des systèmes Ethernet. La norme 10BASE2, qui utilise un câble coaxiale plus fin, a été introduite en 1985. La norme 10BASE-T (fil en cuivre à paires torsadées) est apparue en 1990. Cette dernière, qui comptait plusieurs fils, permit une signalisation en mode full duplex. La technologie 10BASE-T prend en charge un trafic de 10 Mbits/s en mode half-duplex et de 20 Mbits/s en mode full duplex.

La longueur sans répéteur des liaisons 10BASE-T peut atteindre 100 m. Au-delà, les équipements de réseau, tels que les répéteurs, les concentrateurs, les ponts ou les commutateurs, permettent d'accroître l'étendue du LAN. Avec l'apparition des commutateurs, la règle des 4 répéteurs est apparue moins adaptée. Grâce aux commutateurs en chaîne, il est possible d'étendre un LAN indéfiniment. Chaque connexion de commutateur à commutateur, avec une longueur maximale de 100 m, constitue en fait une connexion de bout en bout sans les conflits d'accès aux médias ni les problèmes de synchronisation liés à l'utilisation de répéteurs et de concentrateurs.

La technologie Ethernet 100 Mbits/s, ou Fast Ethernet, peut être mise en œuvre à l'aide d'un fil en cuivre à paires torsadées (100BASE-TX, par exemple) ou avec un média à fibre optique (100BASE-FX, par exemple). Les réseaux Ethernet 100 Mbits/s peuvent offrir un débit de 200 Mbits/s en mode full duplex.

La fréquence plus élevée des signaux Fast Ethernet augmentant le risque de bruit, deux étapes de codage distinctes sont utilisées par l'Ethernet 100 Mbits/s pour améliorer l'intégrité du signal.

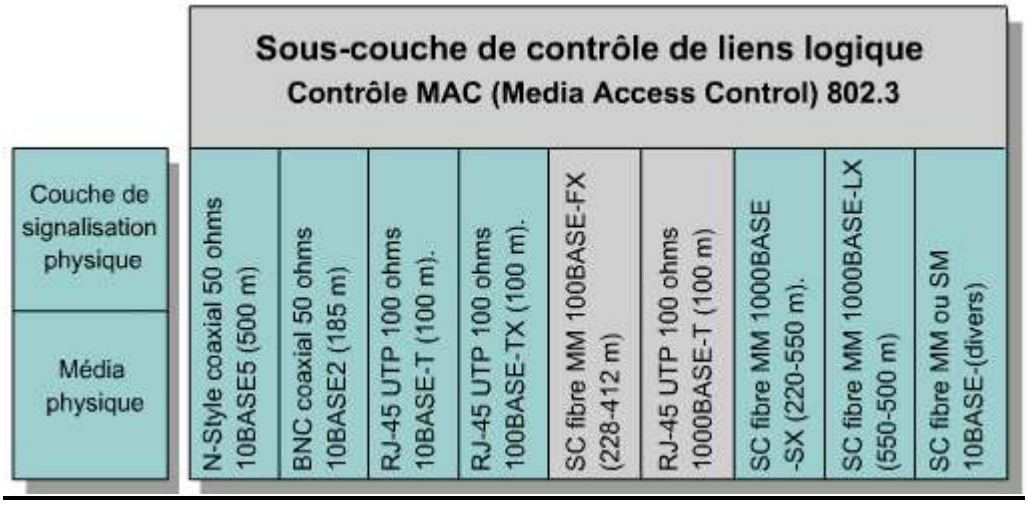
La technologie Gigabit Ethernet avec un câblage en cuivre est mise en œuvre de la façon suivante :

- Un câblage UTP de catégorie 5e et des améliorations électroniques prudentes permettent de passer d'un débit de 100 à 125 Mbits/s par paire de fils.
- Les quatre paires de fils sont utilisées, et pas seulement deux d'entre elles. On obtient ainsi débit de 125 Mbits/s, soit 500 Mbits/s pour les quatre paires de fils.

- Des composants électroniques sophistiqués autorisent les collisions permanentes sur chaque paire de fil et exécutent les signaux en mode full duplex, doublant ainsi le débit (de 500 à 1 000 Mbits/s).

Sur les réseaux Gigabit Ethernet, les signaux binaires se produisent en un dixième du temps des réseaux à 100 Mbits/s et en un centième du temps des réseaux à 10 Mbits/s. La fréquence des signaux étant plus élevée, les bits risquent plus de générer du bruit. Le problème consiste alors à déterminer à quelle vitesse la carte ou l'interface réseau peut modifier les niveaux de tension pour émettre les signaux binaires de telle sorte qu'ils soient détectés de façon fiable à une distance de 100 mètres, au niveau de l'interface ou de la carte réseau du récepteur. À cette vitesse, le codage et le décodage des données deviennent encore plus complexes.

Les versions à fibre optique des systèmes Gigabit Ethernet, 1000BASE-SX et 1000BASE-LX présentent les avantages suivants : elles ne génèrent pas de bruit, leur taille est réduite, elles permettent de disposer de bandes passantes plus larges et elles autorisent des distances non répétées plus grandes. La norme IEEE 802.3 recommande d'utiliser la norme Gigabit Ethernet sur des fibres optiques pour le backbone.


Sous-couche de contrôle de liens logique
Contrôle MAC (Media Access Control) 802.3
Couche de signalisation physique
Média physique
N-Style coaxial 50 ohms 10BASE5 (500 m)
BNC coaxial 50 ohms 10BASE2 (185 m)
RJ-45 UTP 100 ohms 10BASE-T (100 m).
RJ-45 UTP 100 ohms 100BASE-TX (100 m).
SC fibre MM 100BASE-FX (228-412 m)
RJ-45 UTP 100 ohms 1000BASE-T (100 m)
SC fibre MM 1000BASE -SX (220-550 m).
SC fibre MM 1000BASE-LX (550-500 m)
SC fibre MM ou SM 10BASE-(divers)

8-Commutation ethernet

Vue d'ensemble

Un réseau Ethernet partagé fonctionne parfaitement dans des conditions optimales d'utilisation. Lorsque le nombre des équipements qui tentent d'accéder au réseau est peu élevé, le nombre de collisions se maintient à un niveau acceptable. En revanche, lorsque le nombre des utilisateurs augmente, le nombre croissant de collisions peut considérablement réduire les performances du réseau. On peut alors remédier à ce problème en installant des ponts ou encore des commutateurs. Ces derniers, issus de la technologie des ponts, se sont progressivement imposés comme la norme dans les nouveaux réseaux LAN Ethernet.

Les problèmes de broadcast et de collision sont des événements connus dans les réseaux modernes. Malgré leur prise en compte lors de la conception des technologies de couche supérieure et d'Ethernet, les performances du réseau sont amoindries lorsque ces problèmes deviennent trop importants. Afin d'en limiter les effets, des domaines de collision et de broadcast doivent être créés. Ce module passe en revue les répercussions des collisions et des broadcasts sur le trafic d'un réseau, puis il décrit les modalités d'utilisation des ponts et des routeurs pour segmenter un réseau et améliorer les performances.

Ce module se rapporte à des objectifs spécifiques des examens de certification CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Conception et support	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco			• Description du processus " Spanning Tree "

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Conception et support	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception ou modification d'un LAN simple à l'aide de produits Cisco • Design a simple internetwork using Cisco products			• Description du processus " Spanning Tree "

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Comparaison entre les domaines de collision et ceux de broadcast et description du processus de segmentation de réseau • Description des principes et de la mise en pratique de la commutation dans un réseau Ethernet • Explication des méthodes de détection et de gestion des collisions dans un système Ethernet • Explication des concepts fondamentaux associés à la technique d'accès au média Ethernet • Description des principes et de l'usage de la commutation de paquets utilisant le protocole IP (Internet Protocol) • Description du matériel et des logiciels requis pour pouvoir communiquer via un réseau

À l'issue de ce module, les étudiants seront en mesure d'effectuer les actions suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
8.1	Commutation Ethernet
8.2	Domaines de collision et de broadcast

- Définir les notions de pontage et de commutation.
- Définir et décrire une table de mémoire associative (CAM, *Content Addressable Memory*).
- Définir le temps de latence.
- Présenter les modes de commutation par paquets «Store and Forward » et « Cut-through».

- Expliquer le protocole d'acheminement STP (*Spanning-Tree Protocol*).
- Définir les collisions, les broadcasts et les domaines correspondants.
- Identifier les équipements de couche 1, 2 et 3 utilisés pour créer les domaines de collision et de broadcast.
- Aborder la question du flux de données et les problèmes liés au broadcast.
- Décrire la segmentation de réseau et répertorier les équipements utiles à la création de segments.

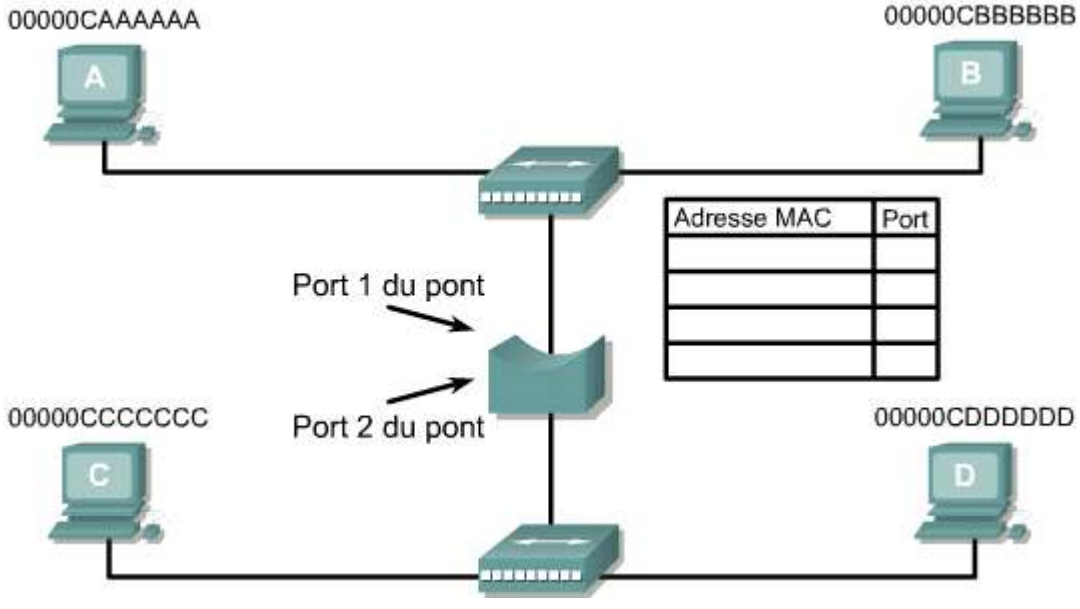
8.1 Commutation Ethernet

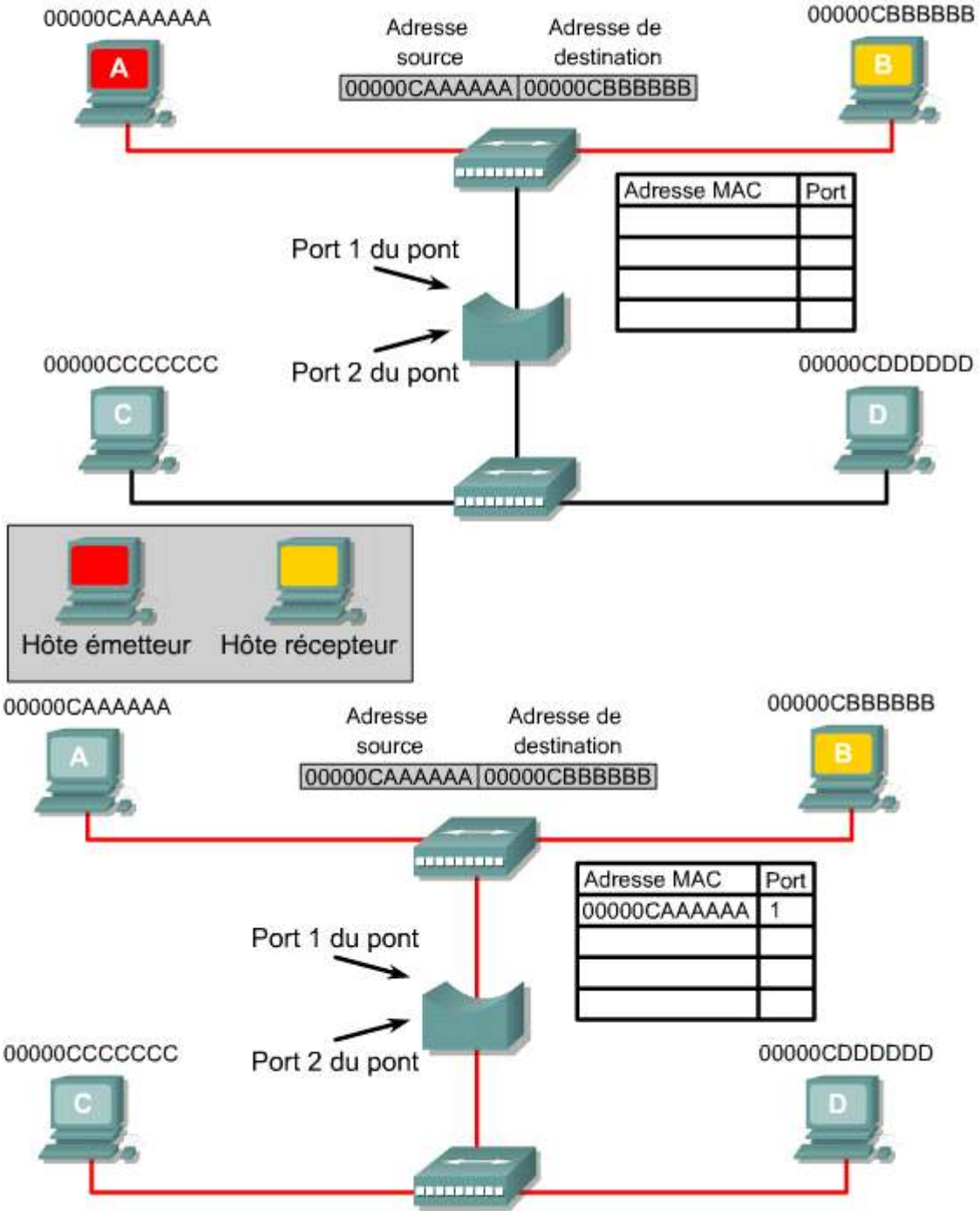
8.1.1 Pontage au niveau de la couche 2

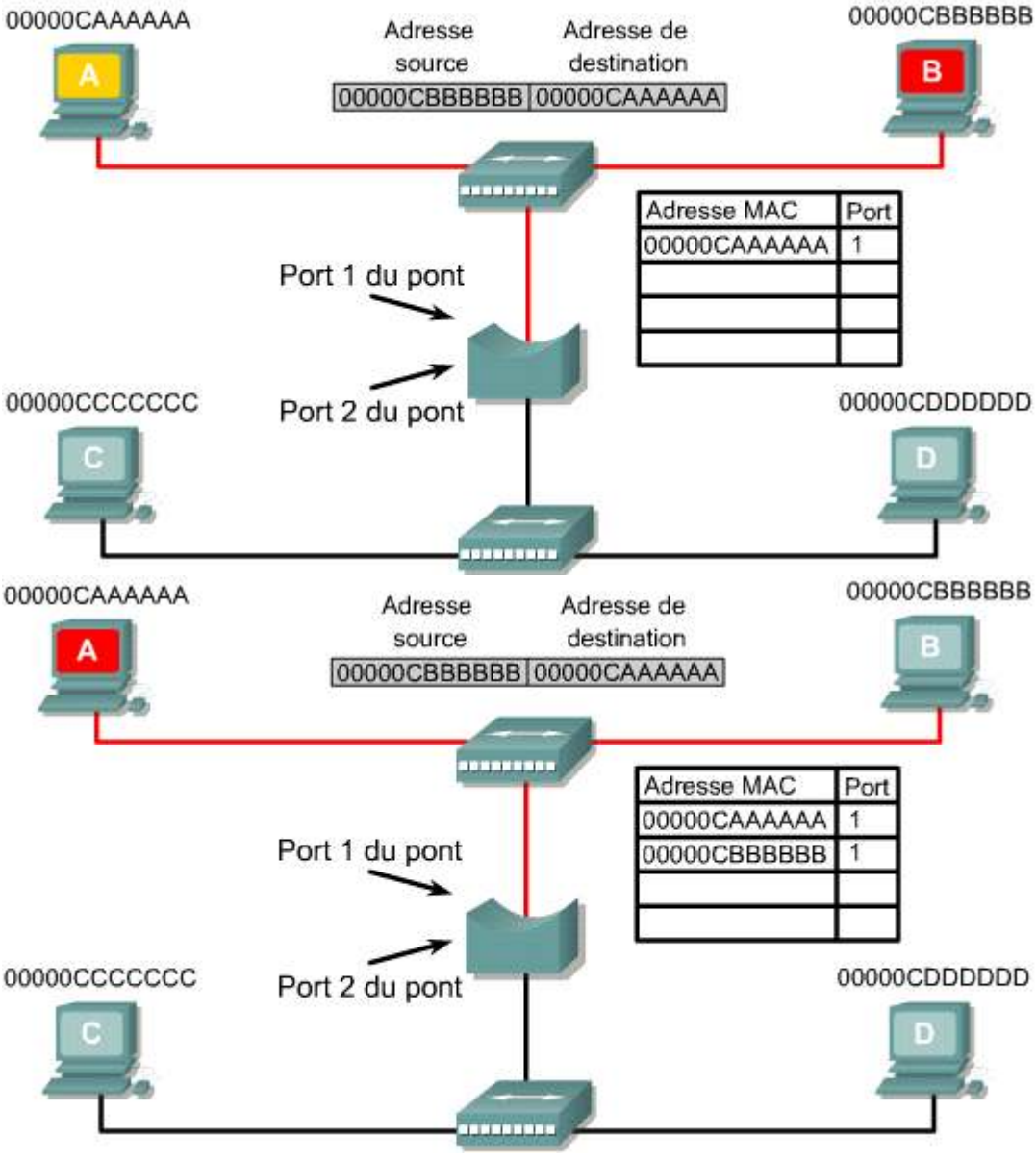
Cette page décrit la procédure de création de ponts au niveau de la couche 2.

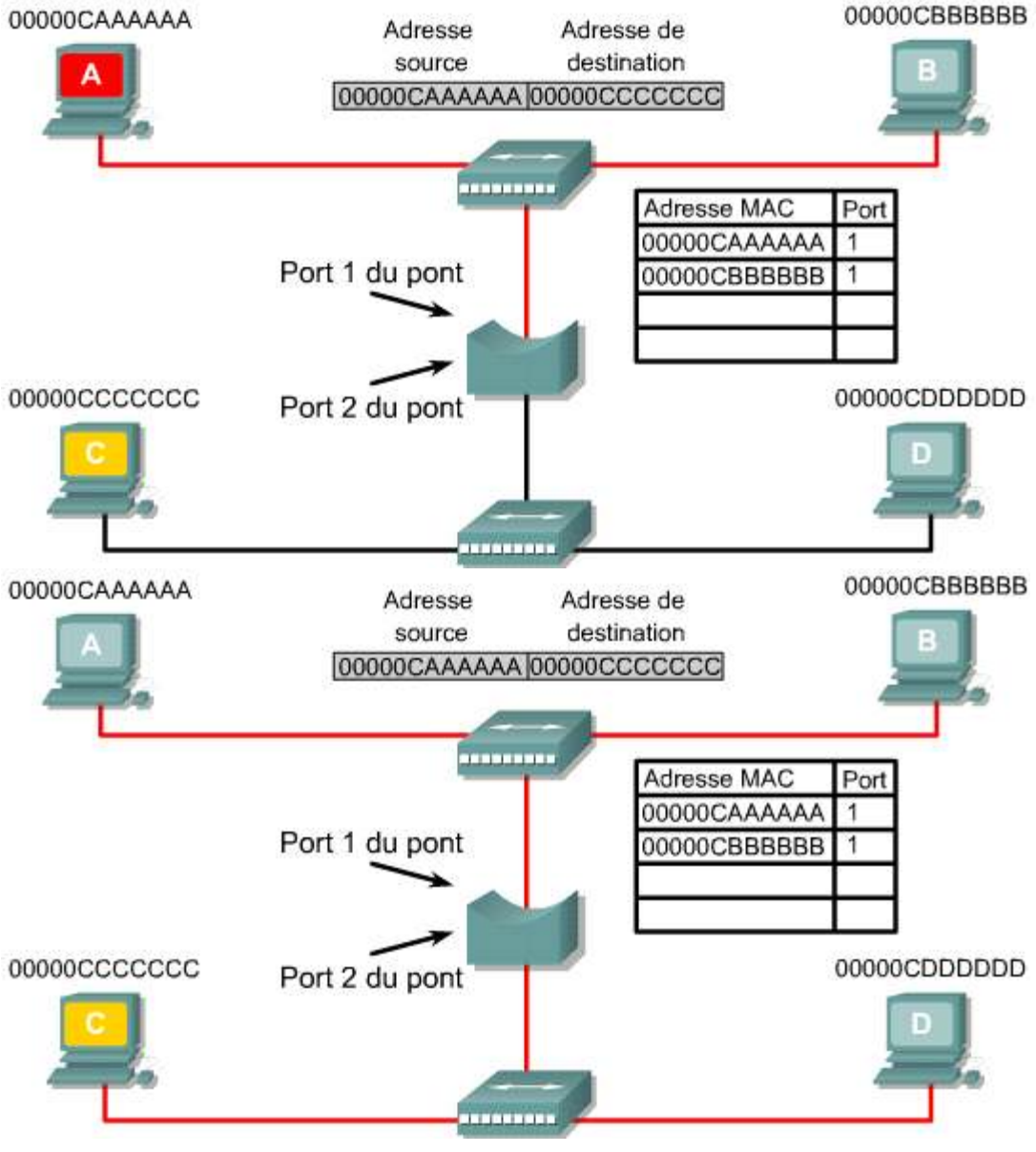
Plus le nombre de nœuds situés sur un segment Ethernet augmente, plus le média est utilisé. Ethernet étant un média partagé, un seul nœud à la fois peut transmettre des données. L'ajout de nœuds entraîne un besoin croissant de bande passante et occasionne des charges supplémentaires sur le média. En outre, la probabilité de collisions est plus forte, ce qui entraîne davantage de retransmissions. L'une des solutions consiste à fragmenter le segment principal en plusieurs parties et à le diviser en domaines de collision distincts.

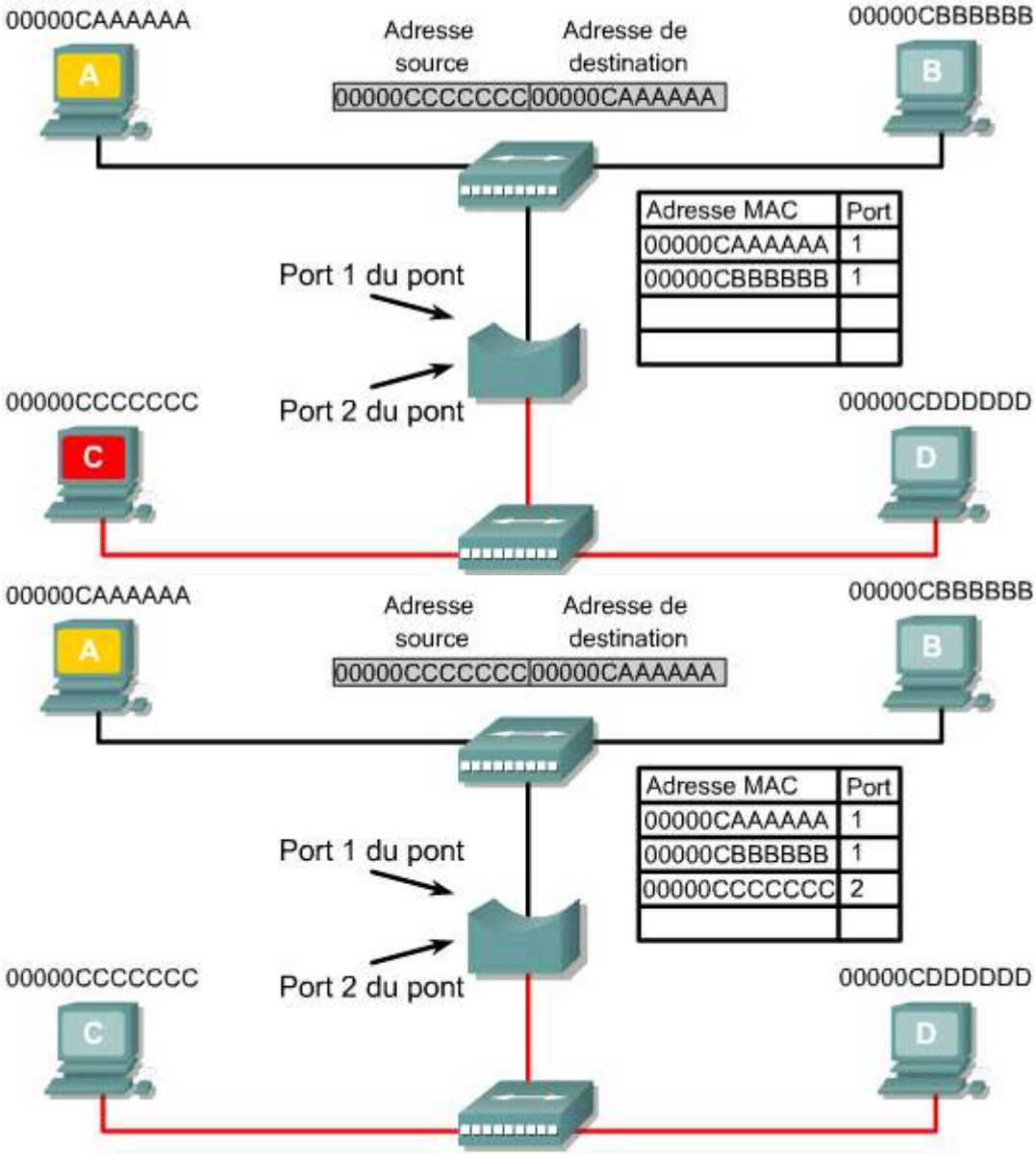
Pour ce faire, on utilise un pont qui établira une table de correspondance entre les adresses MAC et les ports associés. Le pont transmet ensuite les trames, ou les rejette, en fonction des entrées de la table. Voici le fonctionnement d'un pont: [1]

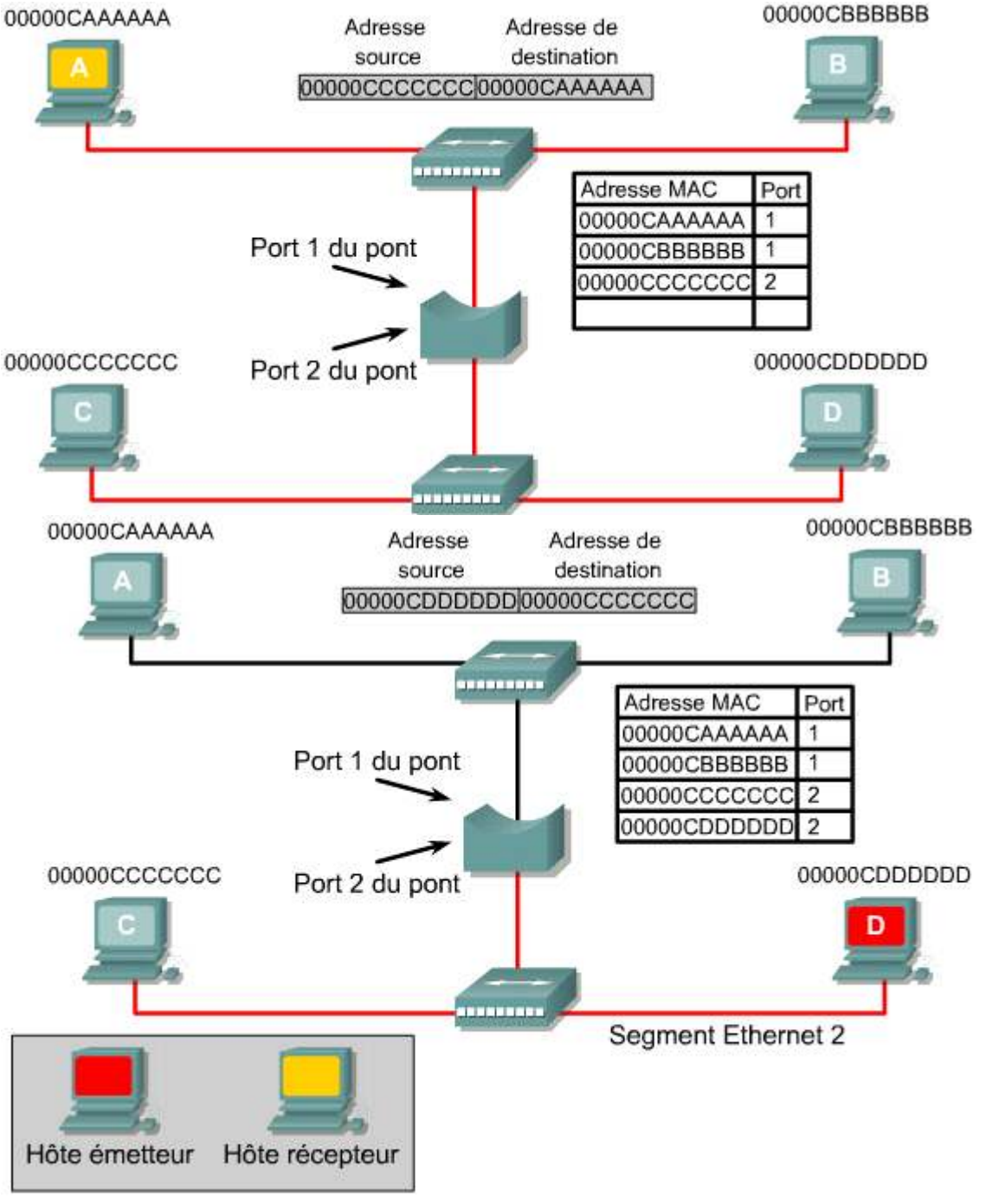



00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CAAAAAA
00000CBBBBBB
A
B
Adresse MAC
Port
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D
Hôte émetteur
Hôte récepteur
00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CAAAAAA
00000CBBBBBB
A
B
Adresse MAC
Port
00000CAAAAAA
1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D


00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CBBBBBB 00000CAAAAAA
A
B
Adresse MAC
Port
00000CAAAAAA 1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D
00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CBBBBBB 00000CAAAAAA
A
B
Adresse MAC
Port
00000CAAAAAA 1
00000CBBBBBB 1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D


00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CAAAAAA
00000CCCCCCC
A
B
Adresse MAC
Port
00000CAAAAAA
1
00000CBBBBBB
1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D
00000CAAAAAA
Adresse source
Adresse de destination
00000CBBBBBB
00000CAAAAAA
00000CCCCCCC
A
B
Adresse MAC
Port
00000CAAAAAA
1
00000CBBBBBB
1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D


00000CAAAAAA
Adresse source
Adresse de destination
00000CCCCCCC
00000CAAAAAA
00000CBBBBBB
A
B
Adresse MAC
Port
00000CAAAAAA
1
00000CBBBBBB
1
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D
00000CAAAAAA
Adresse source
Adresse de destination
00000CCCCCCC
00000CAAAAAA
00000CBBBBBB
A
B
Adresse MAC
Port
00000CAAAAAA
1
00000CBBBBBB
1
00000CCCCCCC
2
Port 1 du pont
Port 2 du pont
00000CCCCCCC
00000CDDDDDD
C
D



- Lorsqu'un pont vient d'être installé, sa table est vide. Le pont attend le transfert de données sur le segment. Dès qu'une transmission est détectée, le pont la traite.
- L'hôte A émet une requête ping vers l'hôte B. Les données étant transmises sur l'ensemble du segment de domaine de collision, le pont et l'hôte B traitent le paquet.
- Le pont ajoute l'adresse source de la trame à sa table de pontage. Sachant que l'adresse se trouve dans le champ d'adresse source et que la trame est reçue sur le port 1, la trame doit être associée au port 1 dans la table.
- L'adresse de destination de la trame est comparée à toutes les adresses de la table de pontage. Bien que les deux adresses se trouvent dans le même domaine de collision, si l'adresse de destination ne se

trouve pas dans la table, la trame est transférée vers le segment suivant. L'adresse de l'hôte B n'est pas encore enregistrée.

- L'hôte B traite la requête ping et transmet la réponse à l'hôte A. Les données sont alors transmises à l'ensemble du domaine de collision. L'hôte A et le pont reçoivent la trame et procèdent à son traitement.
- Le pont ajoute l'adresse source de la trame à sa table de pontage. Sachant que l'adresse source ne se trouve pas dans la table de pontage et qu'elle a été reçue sur le port 1, l'adresse source de la trame doit être associée au port 1 dans la table.
- L'adresse de destination de la trame est comparée à toutes les adresses de la table de pontage afin de vérifier si elle s'y trouve. L'adresse étant dans la table, le numéro de port est vérifié. L'adresse de l'hôte A est associée au port sur lequel la trame a été reçue. Par conséquent, la trame n'est pas transmise.
- L'hôte A émet une requête ping vers l'hôte C. Les données étant transmises sur l'ensemble du segment de domaine de collision, le pont et l'hôte B traitent la trame. L'hôte B rejette la trame car elle ne lui était pas destinée.
- Le pont ajoute l'adresse source de la trame à sa table de pontage. L'adresse existant déjà dans la table de pontage, l'entrée est seulement renouvelée.
- L'adresse de destination de la trame est comparée à toutes les adresses de la table de pontage. L'adresse n'étant pas dans la table, la trame est transmise au segment suivant. L'adresse de l'hôte C n'est pas encore enregistrée.
- L'hôte C traite la requête ping et transmet la réponse à l'hôte A. Les données sont alors transmises à l'ensemble du domaine de collision. L'hôte D et le pont reçoivent la trame et procèdent à son traitement. L'hôte D rejette la trame car elle ne lui était pas destinée.
- Le pont ajoute l'adresse source de la trame à sa table de pontage. Sachant que l'adresse se trouve dans le champ d'adresse source et que la trame est reçue sur le port 2, la trame doit être associée au port 2 dans la table.
- L'adresse de destination de la trame est comparée à toutes les adresses de la table de pontage afin de vérifier si elle s'y trouve. L'adresse se trouve dans la table, mais elle est associée au port 1. Par conséquent, la trame est transmise au segment suivant.
- Lorsque l'hôte D transmet les données, son adresse MAC est également enregistrée dans la table de pontage. C'est sur la base de ce principe que le pont contrôle le trafic entre les domaines de collision.

Nous avons examiné les différentes étapes qu'effectue un pont pour transférer ou rejeter les trames qui sont reçues sur l'un de ses ports.

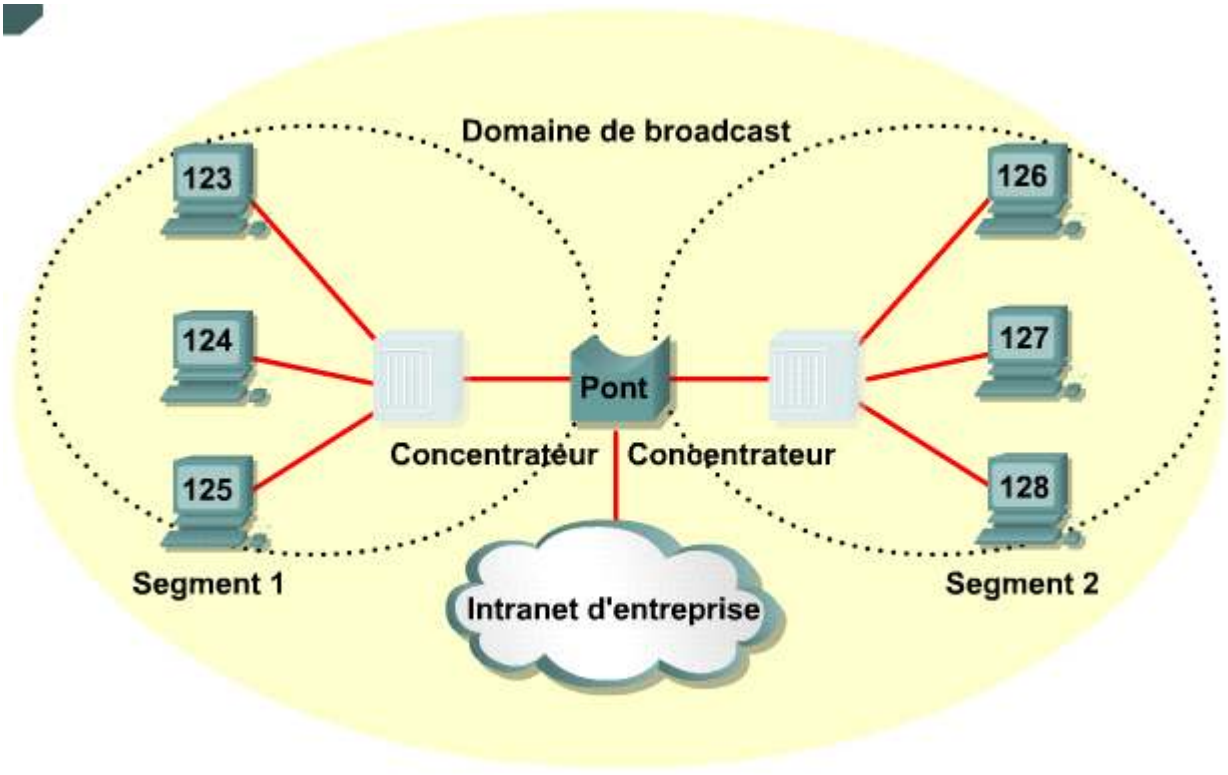
La page suivante traite de la commutation de couche 2.

8.1 Commutation Ethernet

8.1.2 Commutation au niveau de la couche 2

Cette page aborde le principe des commutateurs de couche 2.

En règle générale, un pont comprend deux ports et subdivise un domaine de collision en deux segments. Les décisions prises par un pont dépendent uniquement des adresses MAC (ou adresses de couche 2) et n'affectent pas les adresses de couche 3 (ou adresses logiques). Un pont subdivise un domaine de collision, mais il n'a aucun effet sur le domaine logique ou de broadcast. Si un réseau ne dispose d'aucun équipement relié aux adresses de couche 3, tel qu'un routeur, le réseau tout entier partage le même espace d'adresse de broadcast logique. Un pont crée davantage de domaines de collision, mais n'ajoute pas de domaine de broadcast. 1



Un commutateur est en fait un pont multiport très rapide qui peut contenir des douzaines de ports. Chaque port crée son propre domaine de collision. Lorsqu'un réseau comporte 20 nœuds, 20 domaines de collision doivent exister si chaque nœud est connecté à son propre port de commutation. Dans le cas où un port uplink est installé, un commutateur crée 21 domaines de collision (nœuds uniques). Un commutateur crée et gère de façon dynamique une table de mémoire associative (CAM, *Content Addressable Memory*), qui contient toutes les informations MAC nécessaires aux ports.

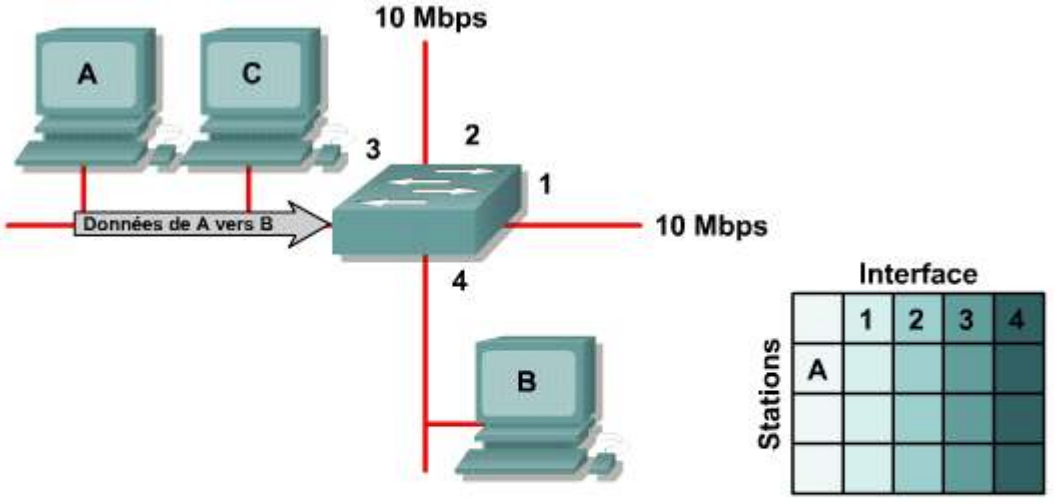
La page suivante explique le fonctionnement d'un commutateur.

8.1 Commutation Ethernet

8.1.3 Fonctionnement d'un commutateur

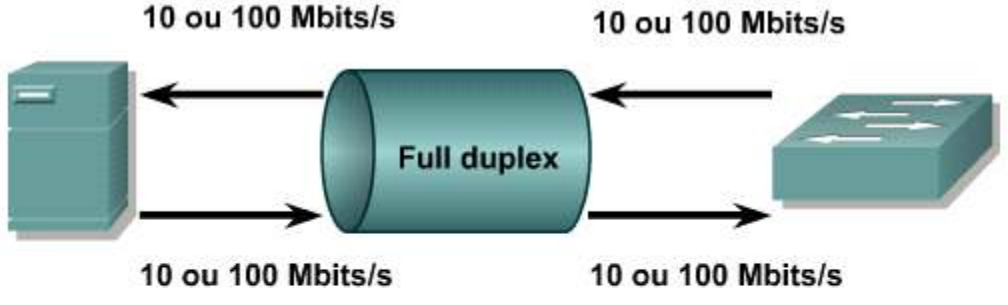
Cette page explique le fonctionnement d'un commutateur.

Un commutateur est un pont doté de plusieurs ports. Lorsqu'un seul nœud est connecté à un port de commutation, le domaine de collision du média partagé ne contient que deux nœuds. Les deux nœuds de ce petit segment, ou domaine de collision, se composent du port de commutation et de l'hôte qui lui est associé. Ces petits segments physiques sont appelés des microsegments. 1



- Transfert de paquets à partir de l'adresse MAC dans la table de transmission
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.

Une nouvelle fonction devient disponible lorsque seulement deux nœuds sont connectés. Dans le cadre d'un réseau basé sur des câbles à paires torsadées, l'une des paires est utilisée pour transmettre le signal d'un nœud à l'autre. L'autre paire permet de recevoir le signal. Les signaux peuvent transiter dans les deux paires simultanément. Une liaison dont les données sont transmises dans les deux sens et simultanément est en mode «full duplex». 2



- Il double la bande passante entre les nœuds.
- Transmission sans collision
- Deux chemins de données à 10 ou 100 Mbits/s

La plupart des commutateurs prennent en charge ce mode full duplex, de même que la plupart des cartes réseau. En mode full duplex, aucun conflit ne se produit au niveau du média. Les domaines de collision n'existent plus. Normalement, l'activation du mode full duplex a pour effet de doubler le volume de la bande passante.

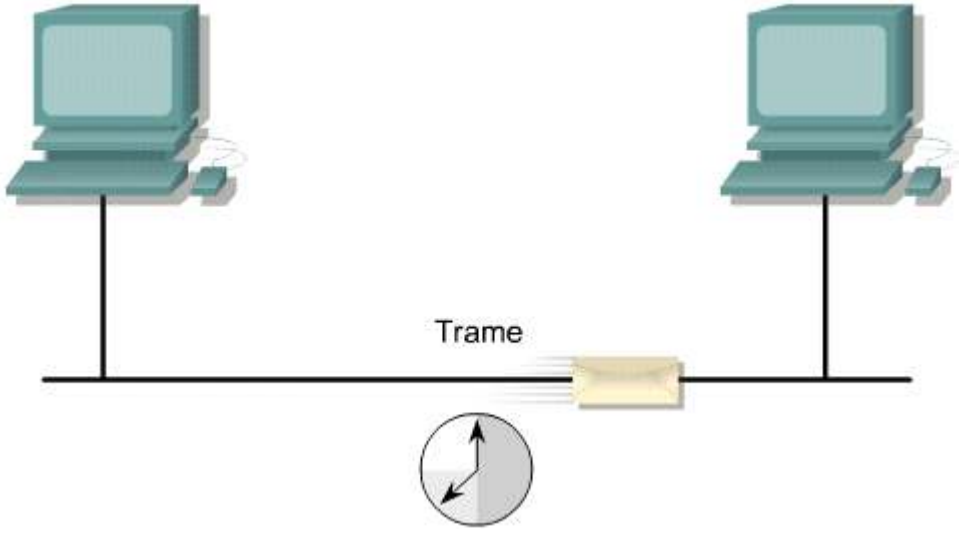
Outre l'apparition de microprocesseurs et de mémoires plus performants, deux autres progrès techniques ont rendu possible le développement des commutateurs. La mémoire CAM effectue l'opération inverse des mémoires traditionnelles. Un contenu est fourni à la mémoire et l'adresse correspondante est récupérée. Cette mémoire permet à un commutateur de rechercher un port associé à une adresse MAC sans algorithme de recherche. Un circuit intégré à application spécifique (ASIC) est un circuit intégré doté de fonctionnalités personnalisées pour un usage particulier (matériel ou projet) et non un usage générique. Un ASIC permet à des fonctions logicielles d'être effectuées de façon matérielle. Ces technologies ont permis de réduire, de façon notable, les retards causés par les processus logiciels. Grâce à elles, les commutateurs ont également pu répondre aux besoins des microsegments en matière de données et de haut débit.

La page suivante définit la notion de latence.

8.1 Commutation Ethernet
8.1.4 Latence

Cette page décrit quelques-unes des situations pouvant provoquer un temps d'attente.

On appelle latence le temps qui s'écoule entre le moment où une trame quitte un équipement source et celui où la première partie de la trame atteint sa destination. 1



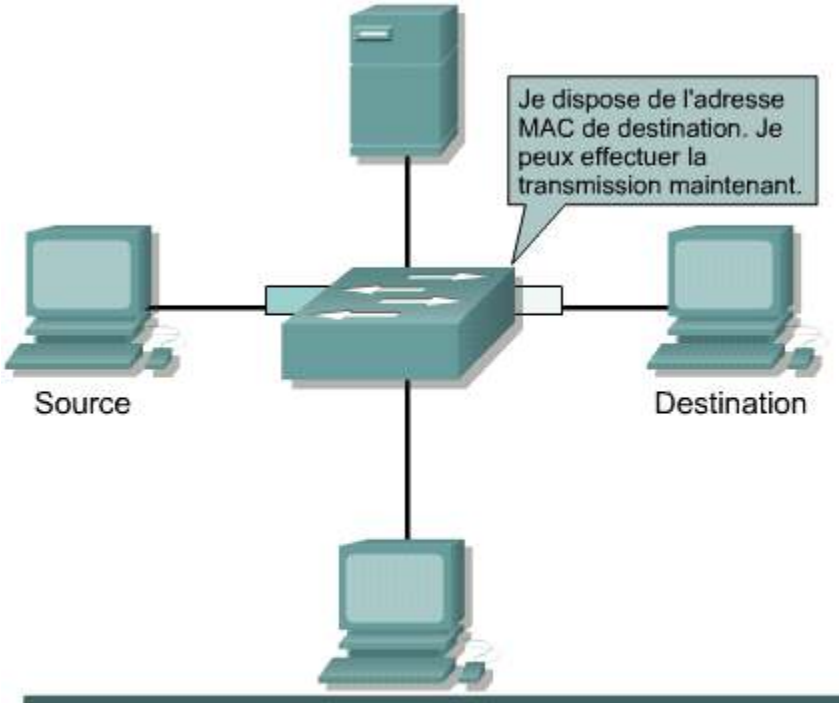
Plusieurs causes peuvent être à l'origine de ces retards:

- Les retards au niveau des médias peuvent être causés par la vitesse finie de propagation des signaux dans le média physique.
- Les retards au niveau des circuits peuvent être causés par les composants électroniques qui traitent le signal tout au long du chemin.
- Les retards au niveau des applications peuvent être causés par les décisions prises par les logiciels pour implémenter la commutation et les protocoles.
- Les retards peuvent être causés par le contenu de la trame et l'emplacement des décisions relatives à la commutation de la trame. Par exemple, un équipement ne peut pas acheminer une trame vers une destination tant que l'adresse MAC de destination n'a pas été identifiée. 1

La page suivante présente les modes de commutation.

Cette page décrit les trois modes de commutation possibles.

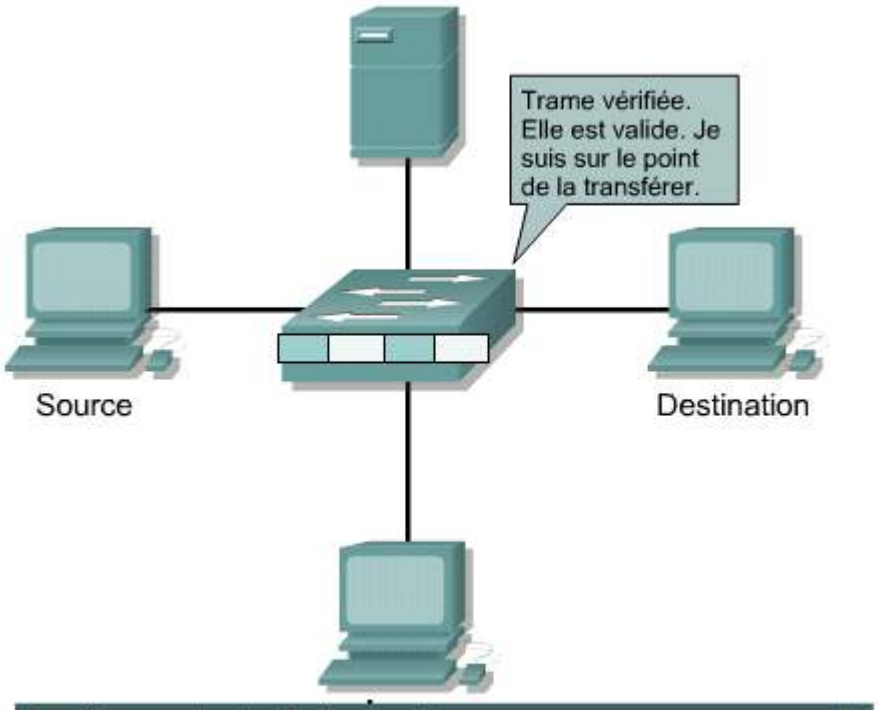
La commutation d'une trame vers un port de destination est fonction du niveau de latence et de fiabilité. Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue. Ce mode de commutation des paquets est appelé «Cut-through»: il se caractérise par un temps de latence très faible. 1



Fenêtre contextuelle (pop up)

Un commutateur de paquets " cut-through " commence à transmettre le paquet au port de destination dès que l'adresse de destination est trouvée dans la table de commutation et que l'interface de sortie est déterminée.

Cependant, la vérification des erreurs n'est pas effectuée. Un commutateur peut également attendre de recevoir la trame entière avant de la transférer vers le port de destination. Cela permet au logiciel de commutation de vérifier la séquence de contrôle de trame (FCS, *Frame Check Sequence*). Si la trame n'est pas correcte, elle est rejetée au niveau du commutateur. Étant donné que la trame entière est stockée avant d'être transmise, ce mode de commutation des paquets est appelé «Store-and-Forward». 2


Trame vérifiée. Elle est valide. Je suis sur le point de la transférer.
Source
Destination
Fenêtre contextuelle (pop up)
Un commutateur " Store-and-Forward " copie toute la trame, effectue le contrôle de redondance cyclique ou CRC et vérifie la longueur de la trame. Si le CRC et la longueur de la trame sont valides, le commutateur examine l'adresse de destination dans sa table, détermine l'interface de sortie et transmet la trame vers sa destination.

Une solution intermédiaire de commutation des paquets est le mode «Fragment-Free». Ce mode lit les 64 premiers octets, incluant l'en-tête de la trame, puis il commence à transmettre le paquet avant même d'avoir terminé la lecture du champ de données et de la somme de contrôle. Ce mode vérifie la fiabilité des adresses et des informations relatives au protocole LLC afin de garantir que les données sont correctement traitées et qu'elles sont acheminées vers la destination appropriée.

Avec le mode de commutation «Cut-through», les débits des ports source et de destination doivent être identiques pour ne pas endommager la trame. On parle alors de commutation symétrique. Lorsque les débits sont différents, la trame utilise un certain débit pour la réception et un autre pour l'émission. C'est ce qu'on appelle une commutation asymétrique. Le mode «Store-and-Forward» doit être utilisé dans le cadre d'une commutation asymétrique.

Cette dernière fournit des connexions commutées entre les ports ayant une bande passante différente. La commutation asymétrique est particulièrement adaptée aux flux de trafic client-serveur où plusieurs clients communiquent avec un serveur simultanément. Une bande passante plus large doit être allouée au port du serveur afin d'éviter qu'un goulot d'étranglement ne se produise au niveau de ce port.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les trois modes de commutation.

La page suivante traite du protocole STP (*Spanning-Tree Protocol*).

Activité de média interactive

Glisser-Positionner: Modes de commutation

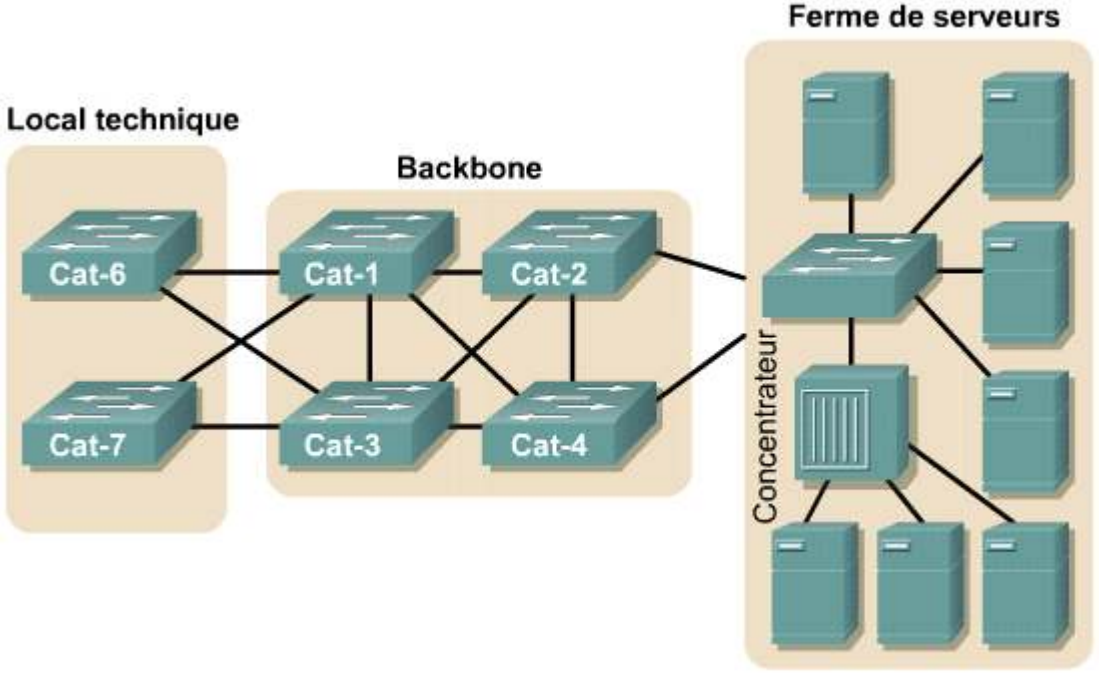
À l'issue de cette activité, les étudiants seront capables d'identifier les trois modes de commutation.

8.1 Commutation Ethernet

8.1.6 Protocole STP (Spanning-Tree Protocol)

Cette page présente le protocole STP.

Lorsque plusieurs commutateurs sont placés dans une arborescence hiérarchique simple, il est peu probable que des boucles de commutation se produisent. Toutefois, les réseaux commutés possèdent très souvent des chemins redondants afin d'assurer une meilleure fiabilité et une meilleure tolérance aux pannes. 1



Bien qu'extrêmement utiles, les chemins redondants peuvent avoir des effets secondaires, tels que les boucles de commutation. Ces boucles de commutation représentent un inconvénient. Elles peuvent survenir intentionnellement ou accidentellement et elles peuvent provoquer des tempêtes de broadcasts qui risquent de submerger rapidement le réseau. Le protocole STP est un protocole normalisé qui permet d'éviter les boucles de commutation. Chaque commutateur d'un réseau LAN qui utilise le protocole STP envoie un message appelé BDPU (*Bridge Protocol Data Unit*) par le biais de tous ses ports afin que les autres commutateurs soient informés de son existence. Les informations contenues dans ce message sont alors utilisées pour désigner le pont racine du réseau. Les commutateurs utilisent l'algorithme «spanning-tree» pour résoudre les chemins redondants.

Chaque port d'un commutateur utilisant le protocole STP a pour état l'un des cinq suivants: 2

États	Objectif
Blocage	Reçoit uniquement les unités BPDU.
Écoute	Construction d'une topologie " active "
Acquisition	Construction d'une table de pontage
Transmission	Envoi et réception de données utilisateur
Désactivation	Désactivation par un administrateur

- Blocage
- Écoute
- Apprentissage
- Acheminement
- Désactivation

Un port change d'état comme suit:

- De l'initialisation au blocage.
- Du blocage à l'écoute ou à la désactivation.
- De l'écoute à l'apprentissage ou à la désactivation.
- De l'apprentissage à l'acheminement ou à la désactivation.
- De l'acheminement à la désactivation.

Le protocole STP permet de créer une arborescence hiérarchique logique sans boucle. Cependant, des chemins de remplacement sont toujours disponibles, si nécessaire.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les fonctions de chaque état des ports «spanning-tree».

Cette page termine la leçon. La leçon suivante présente les domaines de collision et de broadcast. La première page traite des environnements de médias partagés.



Activité de média interactive

Jeu de mots croisés: États «spanning tree»

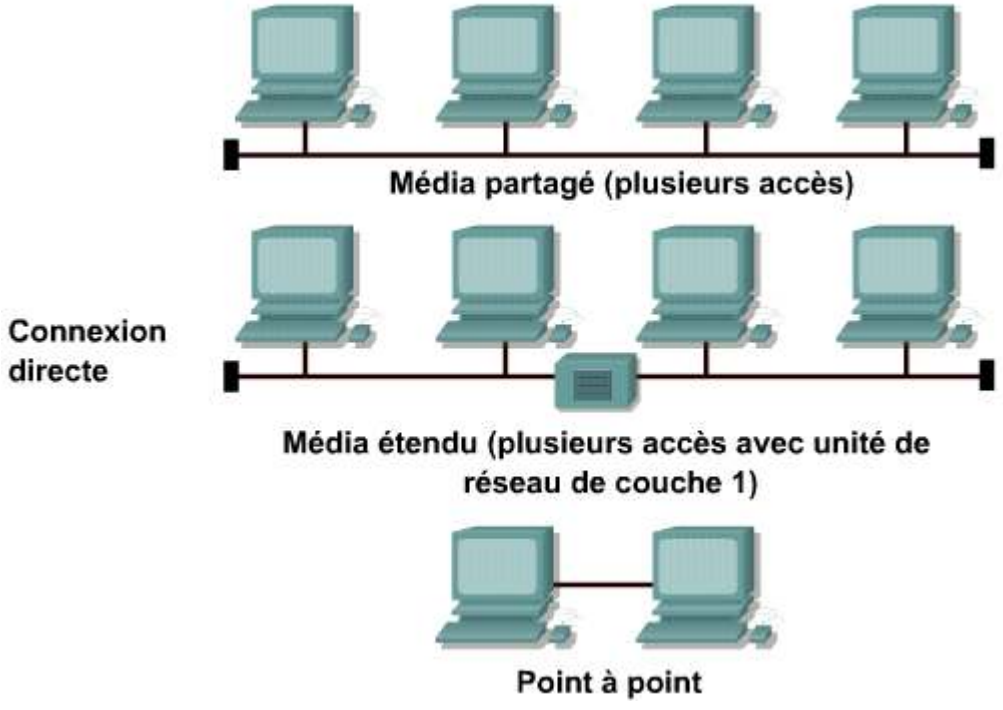
À l'issue de cette activité, les étudiants seront capables d'identifier les fonctions des états «spanning tree».

8.2 Domaines de collision et de broadcast

8.2.1 Environnements de médias partagés

Cette page présente les topologies et médias de la couche 1 afin d'aider les étudiants à mieux appréhender les collisions et les domaines de collision.

Voici quelques exemples de réseaux directement connectés et de médias partagés: 1


Média partagé (plusieurs accès)
Connexion directe
Média étendu (plusieurs accès avec unité de réseau de couche 1)
Point à point

- **Environnement de média partagé:** plusieurs hôtes ont accès au même média. Par exemple, si plusieurs PC sont connectés au même fil physique ou au même câble à fibre optique, ils partagent le même environnement de média.
- **Environnement de média partagé étendu:** type particulier d'environnement de média partagé où des équipements de réseau étendent leur environnement de manière qu'il prenne en charge plusieurs accès ou des câbles plus longs.
- **Environnement de réseau point à point:** environnement réseau très répandu dans les réseaux commutés et chez les télétravailleurs. Il s'agit d'un environnement réseau partagé où un équipement est directement connecté à un seul autre équipement. Un PC connecté à un fournisseur d'accès Internet à l'aide d'une ligne téléphonique et d'un modem en constitue un exemple.

Les collisions ne se produisent que dans les environnements partagés. Le système autoroutier est un exemple d'environnement partagé où des collisions peuvent se produire en raison du nombre de véhicules qui empruntent les mêmes routes. Plus le nombre de véhicules est important, plus le risque de collision est élevé. Un réseau de données partagé fonctionne de la même manière qu'une autoroute. Des règles existent pour déterminer qui a le droit d'accéder au média réseau. Toutefois, il arrive que ces règles ne parviennent pas à traiter la charge de trafic et que des collisions se produisent.

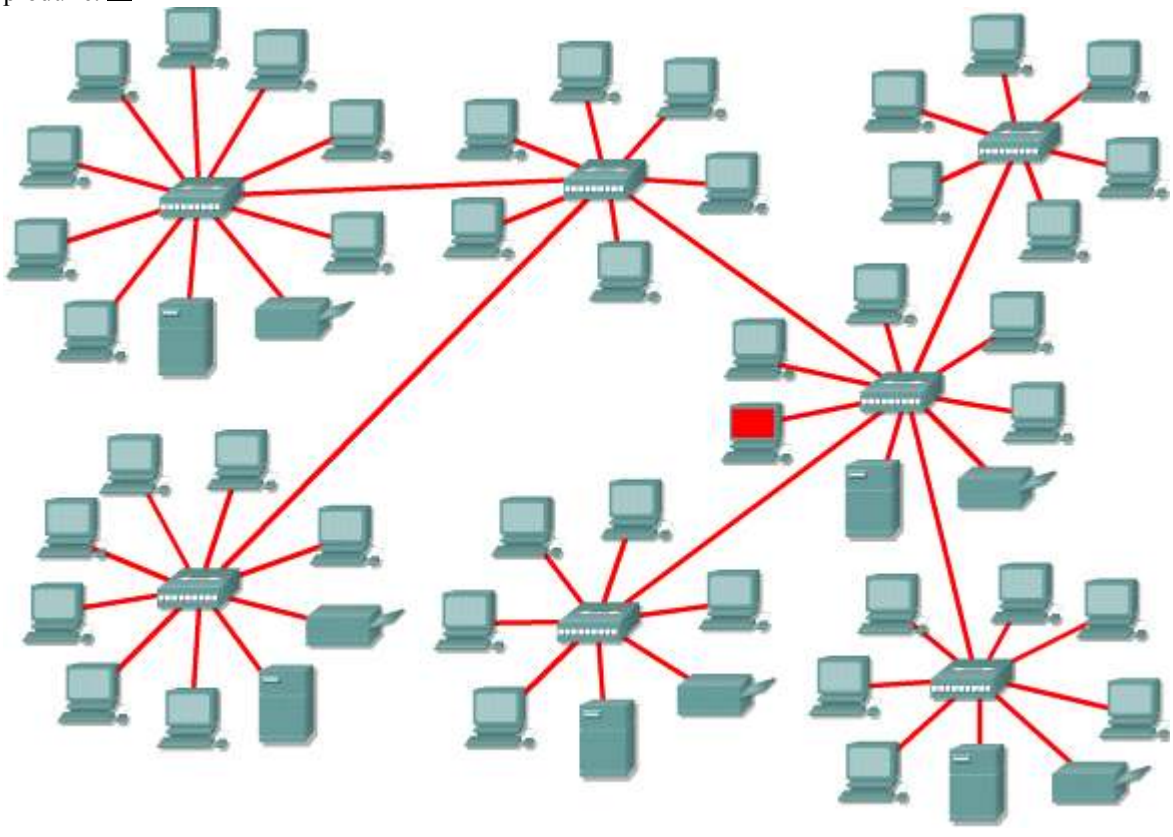
La page suivante porte sur les domaines de collision.

8.2 Domaines de collision et de broadcast

8.2.2 Les domaines de collision

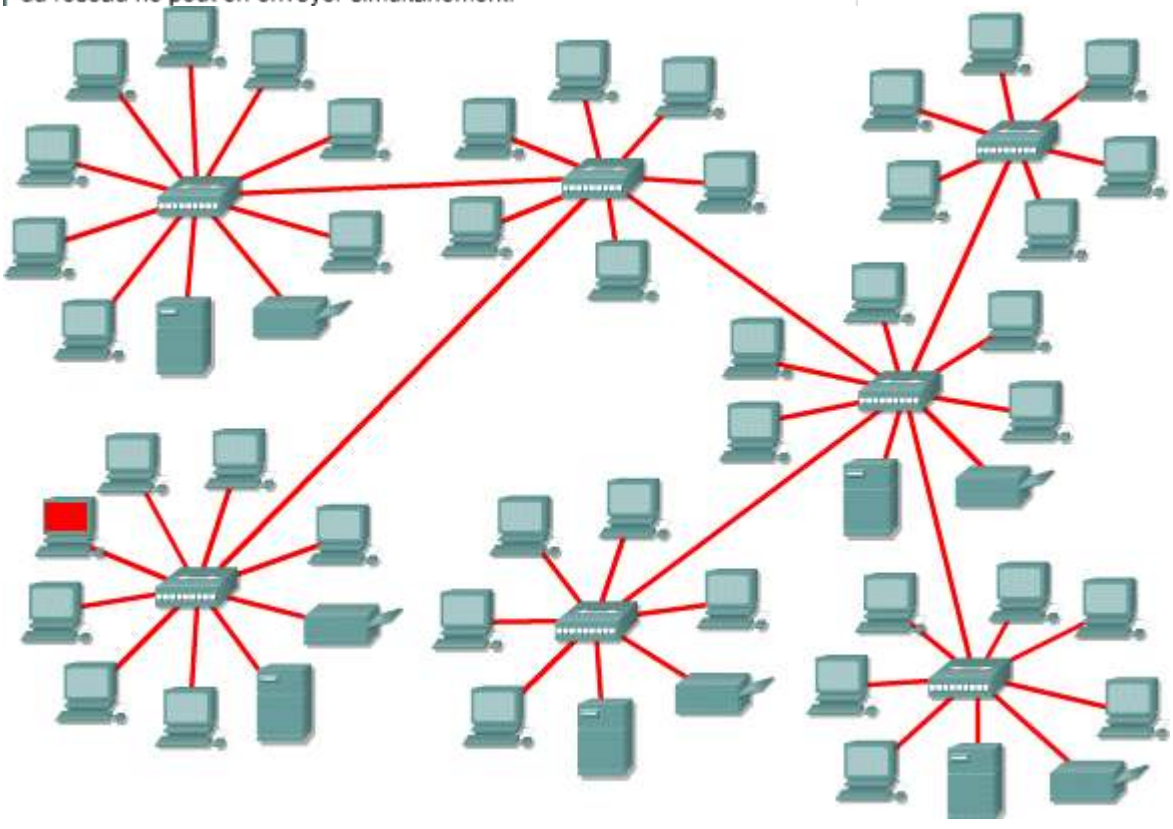
Cette page définit les domaines de collision.

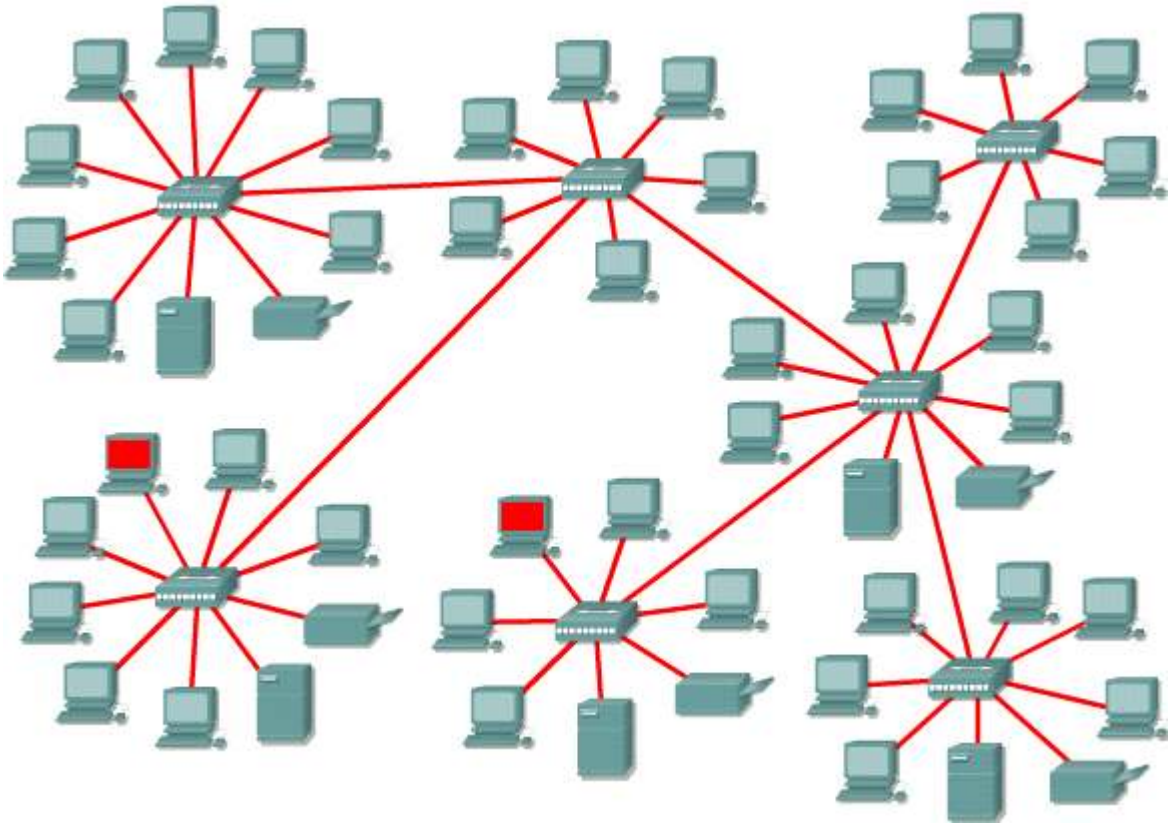
On appelle domaines de collision des segments du réseau physique dans lesquels des collisions peuvent se produire. 1



Fenêtre contextuelle (pop up)

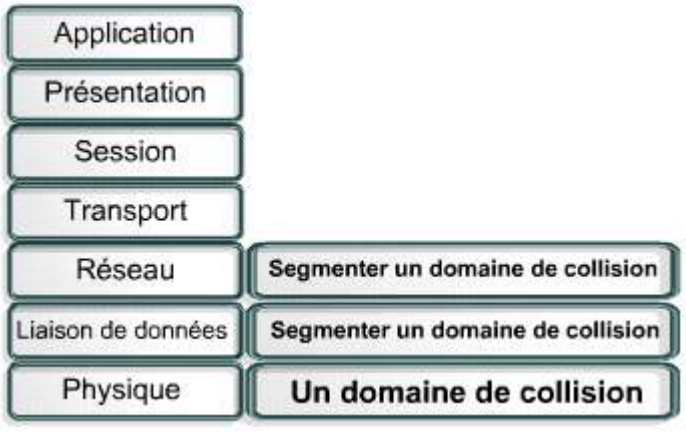
Ce réseau, composé de 43 hôtes, de 5 serveurs, de 5 imprimantes réseau et de 7 concentrateurs, constitue un domaine de collision/de broadcast unique. Lorsqu'un hôte ou un serveur effectue une transmission, tous les autres équipements la reçoivent. Plus important encore, lorsqu'un équipement du réseau envoie des données, aucun des autres équipements du réseau ne peut en envoyer simultanément.





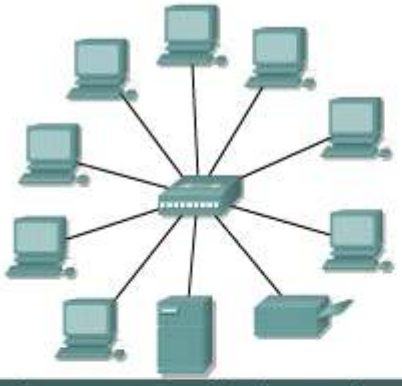
Les collisions rendent le réseau inefficace. Chaque fois qu'une collision survient sur un réseau, les transmissions s'interrompent momentanément. La durée de cette interruption est variable et est fonction d'un algorithme de réémission temporisée pour chaque équipement du réseau.

Les types d'équipements assurant l'interconnexion des segments de médias définissent les domaines de collision. 2



Ces équipements sont des équipements de couche OSI 1, 2 ou 3. Les équipements de couche 2 et 3 segmentent les domaines de collision. Ce processus est d'ailleurs appelé «segmentation».

Les équipements de couche 1, notamment les répéteurs et les concentrateurs, sont principalement utilisés pour étendre les segments de câble Ethernet. 3

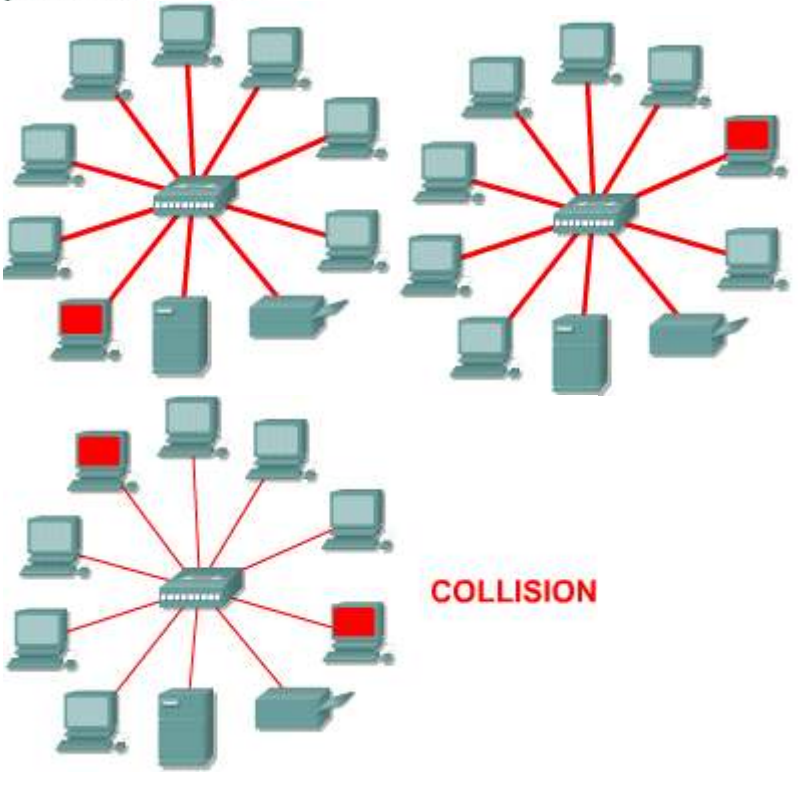


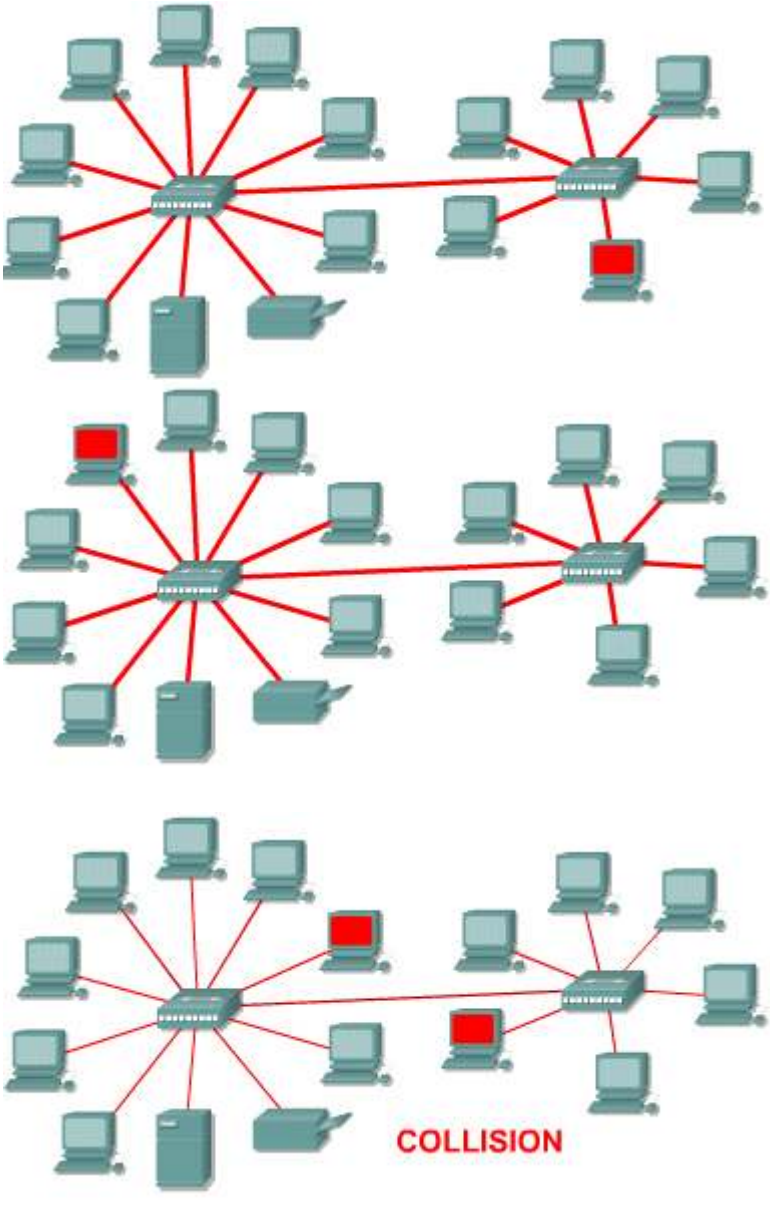
Fenêtre contextuelle (pop up)

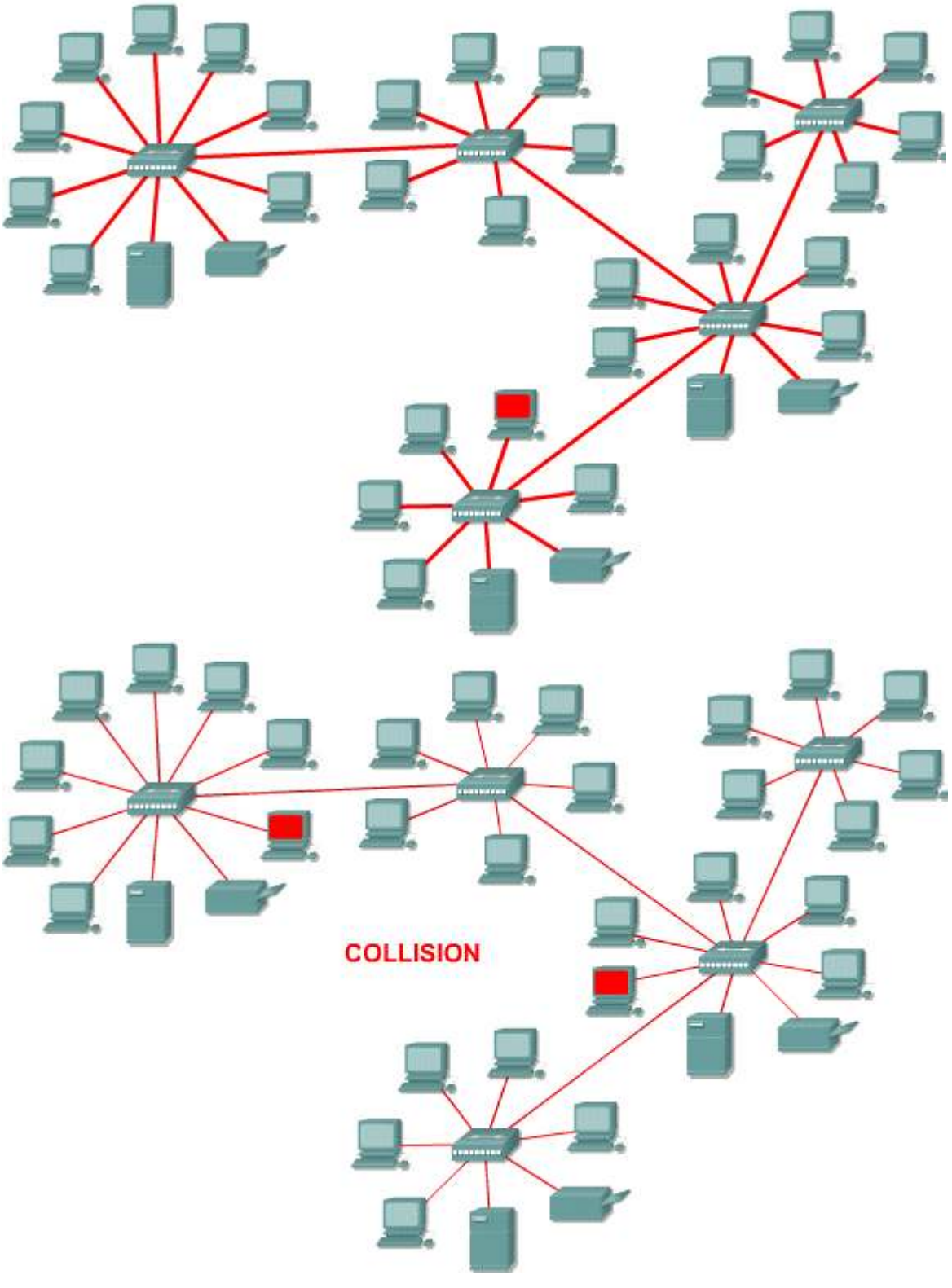
Dans un petit réseau, l'utilisation d'un seul domaine de collision est amplement suffisant, car il existe peu de conflits au niveau du média réseau. Ce type de réseau convient parfaitement pour un réseau isolé qui ne requiert pas beaucoup de transmissions de données.

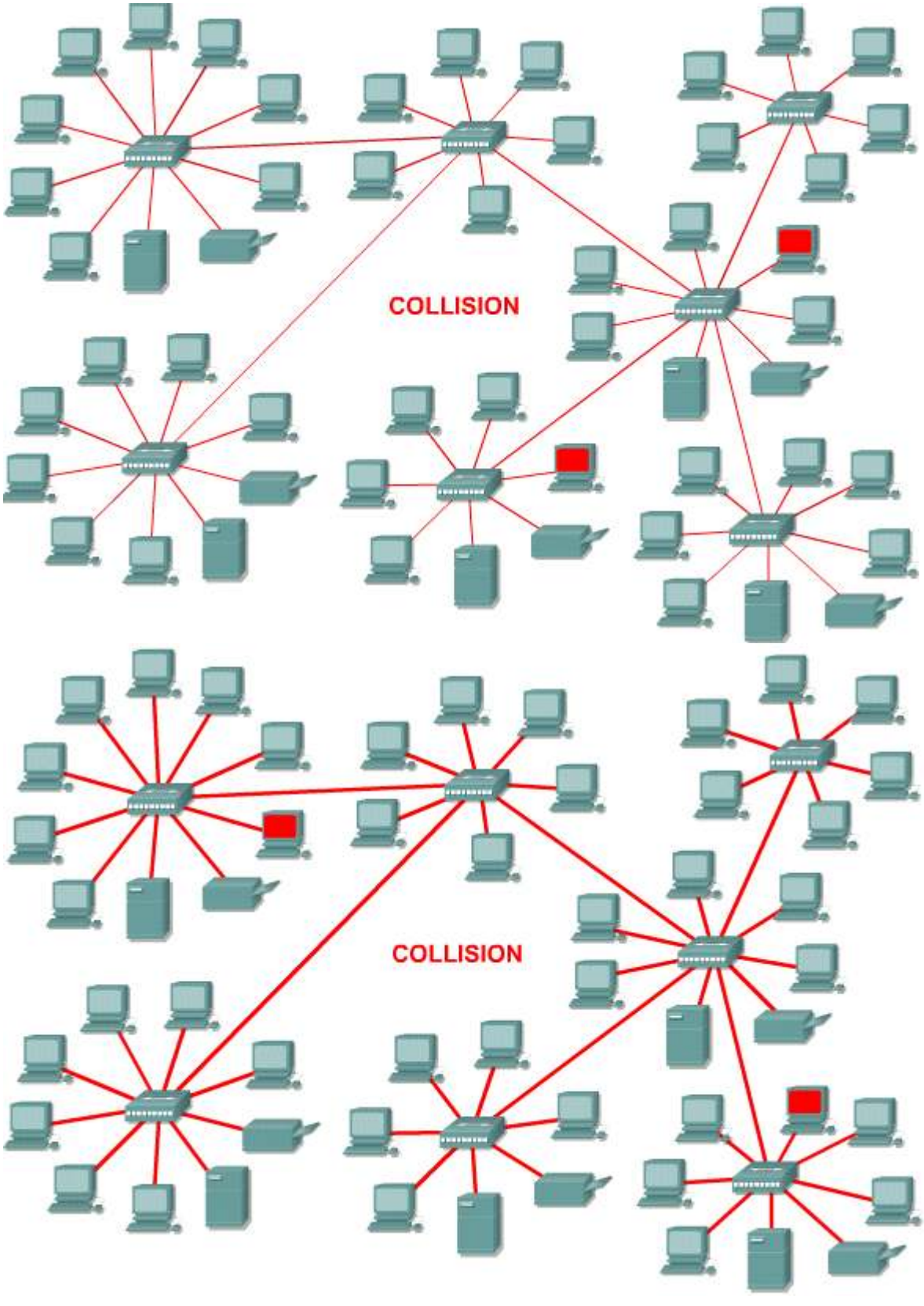
En revanche, plus la taille du réseau croît, plus les conflits au niveau de la ligne deviennent fréquents et plus le nombre de collisions augmente.

Plus le réseau se développe et plus les conflits à l'égard de la ligne deviennent importants, ce qui finit par affecter la performance des ordinateurs du réseau.




COLLISION

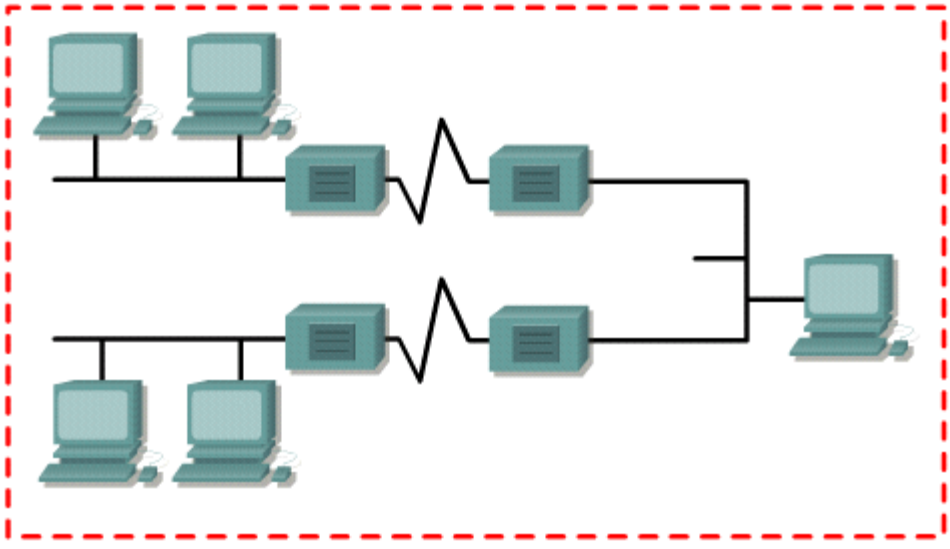

COLLISION



Ils permettent d'ajouter davantage d'hôtes. Cependant, chaque hôte ajouté augmente la quantité de trafic potentiel sur le réseau. Les équipements de couche 1 transmettent la totalité des données qui sont reçues sur le

média. Plus le trafic est dense dans un domaine de collision, plus les risques de collision sont importants. Il en résulte une diminution des performances du réseau, qui sera d'autant plus significative si tous les ordinateurs consomment une grosse quantité de bande passante. Les équipements de couche 1 peuvent être à l'origine de collisions en raison d'une augmentation trop importante du réseau LAN.

La règle des quatre répéteurs Ethernet stipule qu'un maximum de quatre répéteurs ou concentrateurs est autorisé entre deux ordinateurs de réseau. 4



= Domaine de collision

Pour qu'un réseau 10BASE-T faisant appel à des répéteurs fonctionne correctement, le calcul du délai entre deux hôtes est soumis à des conditions. Ainsi, toutes les stations de travail détectent l'ensemble des collisions qui se produisent sur le réseau. La latence des répéteurs, le délai de propagation et la latence des cartes réseau participent à la règle des quatre répéteurs. 5

(délais du répéteur + délais du câble + délais de la carte réseau) x 2 < délai maximal entre deux hôtes
Délais de répéteur 10BASE-T Par répéteur < 2 microsecondes Délais du câble ~ 0,55 microseconde tous les 100 mètres Délais carte réseau ~ 1 microseconde par carte
Le délai maximal entre deux hôtes (durée d'un bit 10BASE-T de 0,1 microseconde x taille minimale d'une trame de 512 bits) est de 51,2 microsecondes.

Pour un câble à paires torsadées non blindées d'une longueur de 500 mètres connecté par 4 répéteurs (ou concentrateurs) et 2 cartes réseau, le délai total serait largement inférieur au délai maximal entre deux hôtes.

La violation de cette règle peut conduire au dépassement du délai maximal. Une collision tardive se produit après la transmission des 64 premiers octets de la trame. Les cartes réseau ne sont pas conçues pour

retransmettre automatiquement les données en cas de collision tardive. Les trames de collision tardive ajoutent un délai appelé «délai de consommation». À mesure que le délai de consommation et la latence augmentent, les performances du réseau se dégradent.

La règle dite de «5-4-3-2-1» requiert que les conditions suivantes soient respectées:

- Cinq segments de média réseau.
- Quatre répéteurs ou concentrateurs.
- Trois segments hôte de réseau;
- Deux sections de liaison sans hôte.
- Un grand domaine de collision.

La règle «5-4-3-2-1» fournit également des consignes pour que le délai maximal entre deux hôtes soit compris dans des limites acceptables.

La page suivante traite de la segmentation.

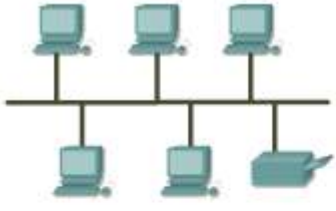
8.2 Domaines de collision et de broadcast
8.2.3 Segmentation

Cette page explique les modalités d'utilisation des équipements de couche 2 et 3 en vue de segmenter un réseau.

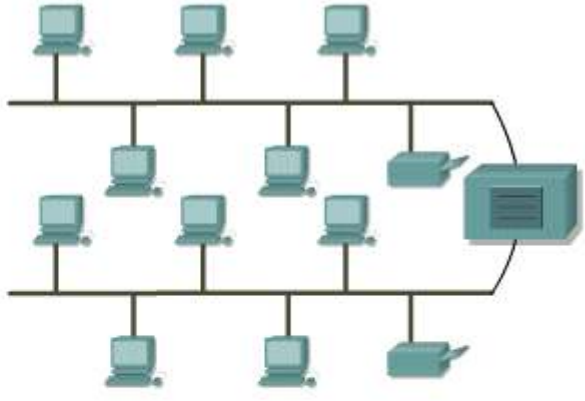
Le traitement Ethernet des collisions et des domaines de collision est né des recherches effectuées par le département de recherche de l'université d'Hawaï en 1970. En voulant concevoir un système de communication sans fil pour les îles Hawaï, les chercheurs de l'université ont créé le protocole Aloha. Le protocole Ethernet est actuellement fondé sur ce protocole.

Un professionnel des réseaux doit savoir reconnaître les domaines de collision. 1

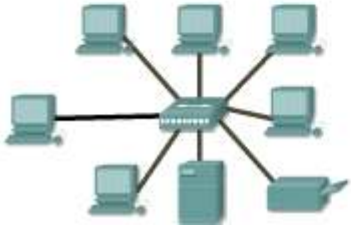
L'accès partagé correspond à un domaine de collision.



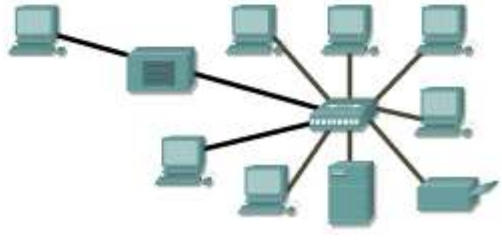
Domaine de collision - étendu par un répéteur



Domaine de collision - créé par un concentrateur

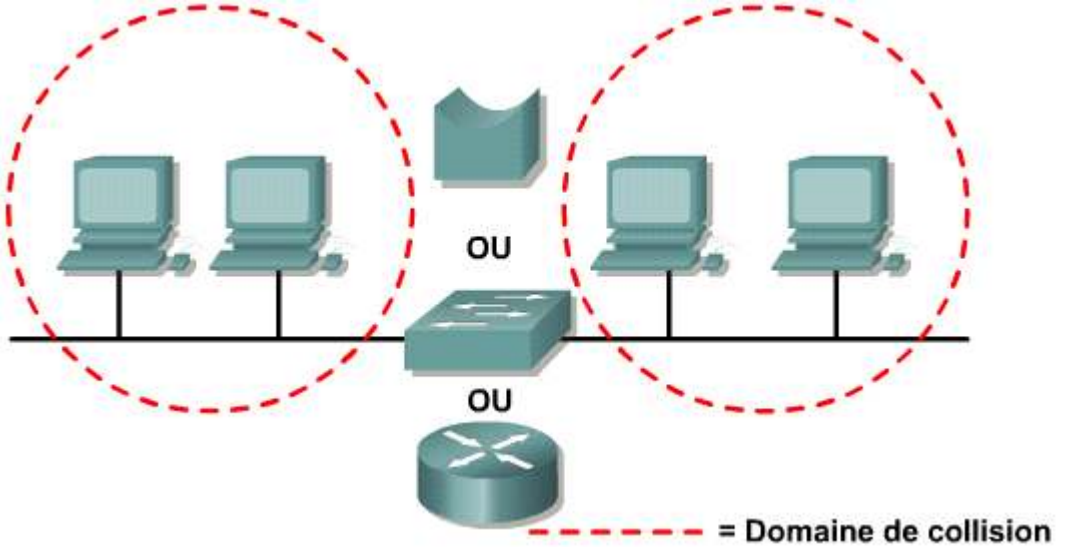


Domaine de collision - étendu par un répéteur



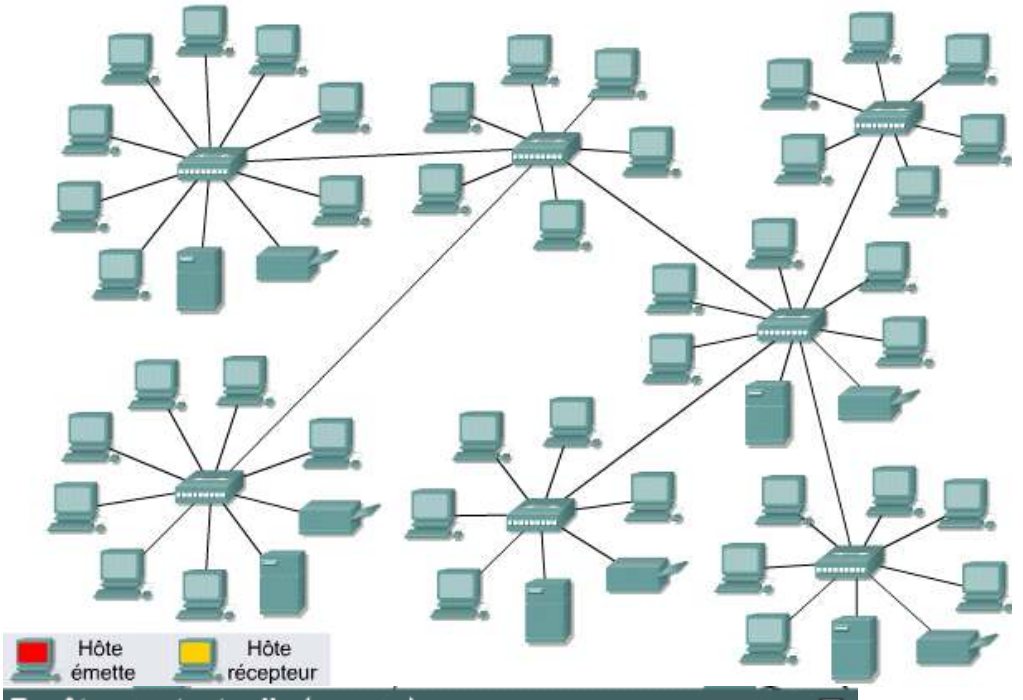
Un domaine de collision est créé lorsque plusieurs ordinateurs sont connectés à un même média partagé qui n'est pas relié aux autres équipements du réseau. Cette situation limite le nombre des ordinateurs qui peuvent utiliser le segment. Les équipements de couche 1 permettent d'étendre les domaines de collision, mais pas de les contrôler.

Les équipements de couche 2 segmentent ou divisent les domaines de collision. 2



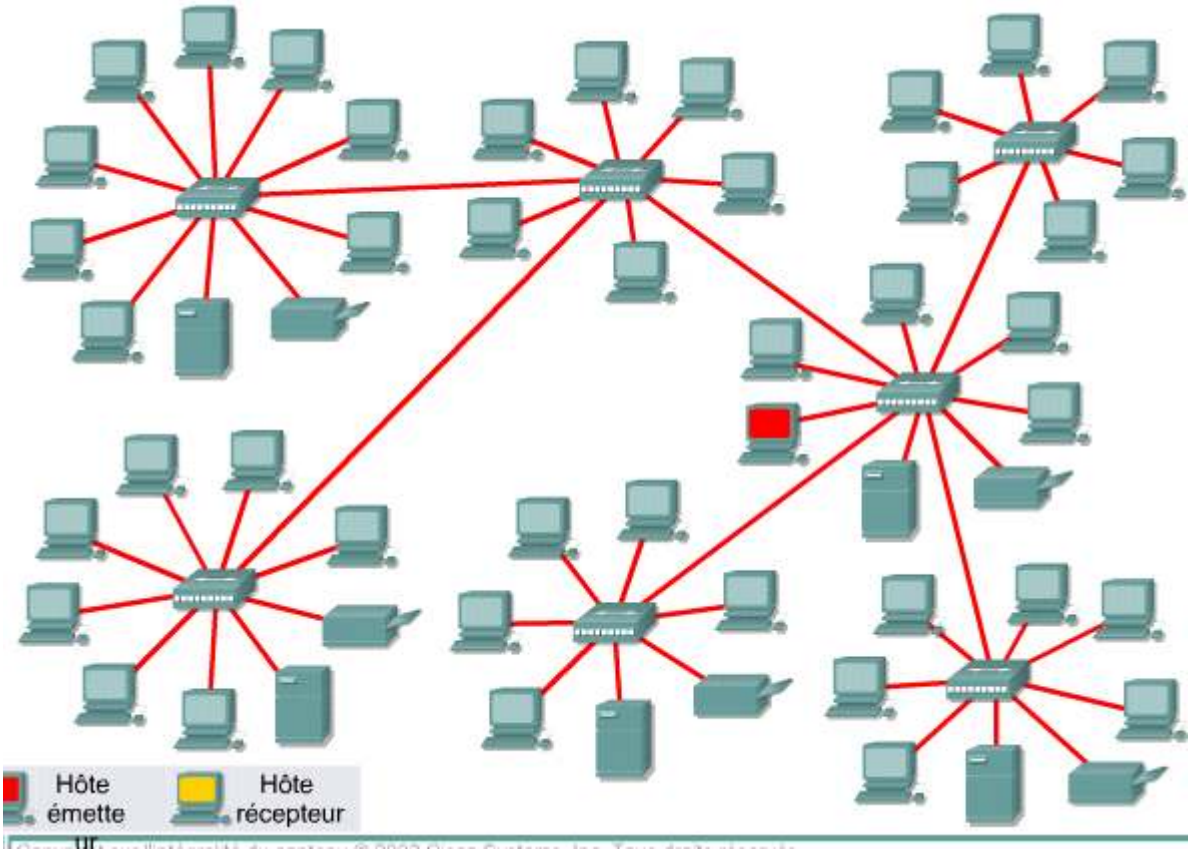
Ils utilisent les adresses MAC affectées à chaque équipement Ethernet pour effectuer le contrôle de propagation de la trame. Les équipements de couche 2 sont des ponts et des commutateurs qui permettent d'effectuer le suivi des adresses MAC et de leurs segments. Ainsi, les équipements peuvent contrôler le flux de trafic au niveau de la couche 2. Grâce à cette caractéristique, les réseaux s'avèrent plus efficaces. Cela permet au réseau de transporter des données simultanément sur différents segments sans collisions. Les ponts et les commutateurs subdivisent les domaines de collision en éléments plus petits. Chaque élément devient alors son propre domaine de collision.

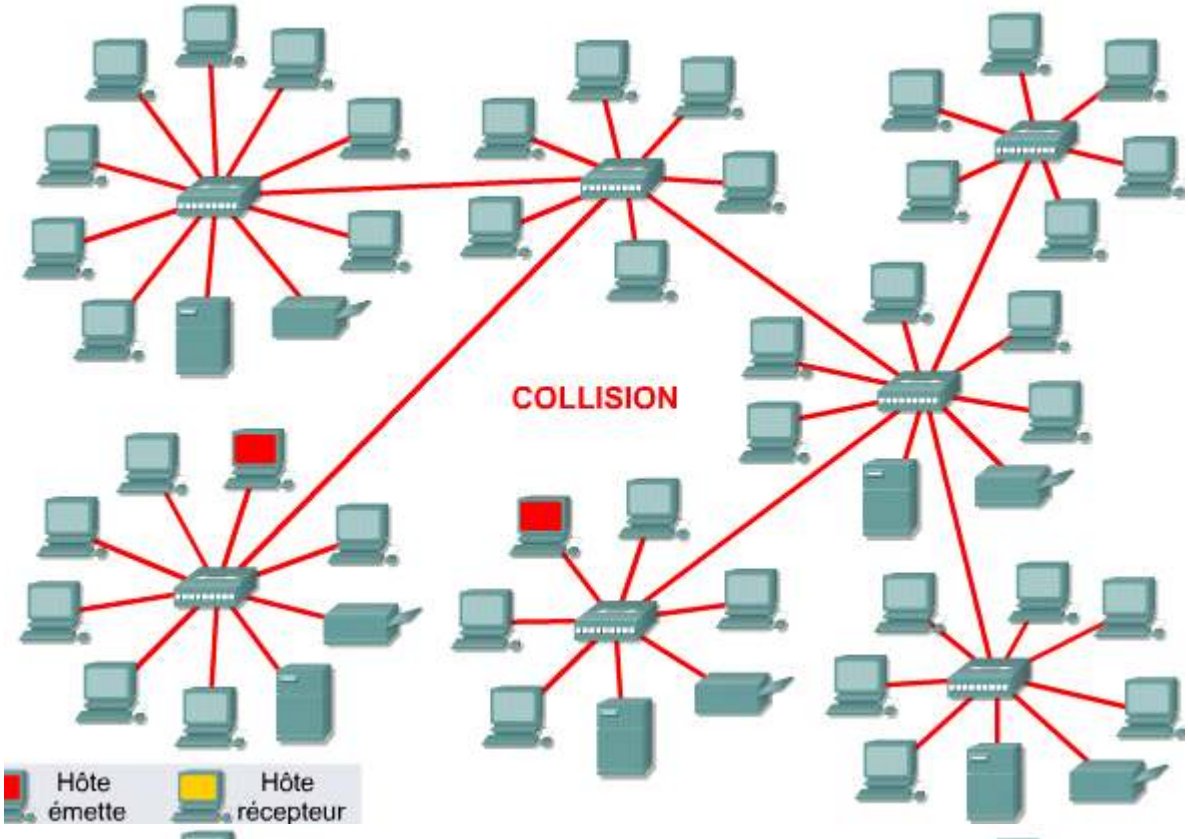
Ces domaines de taille réduite contiennent moins d'hôtes et le trafic est moins dense que dans le domaine d'origine. 3

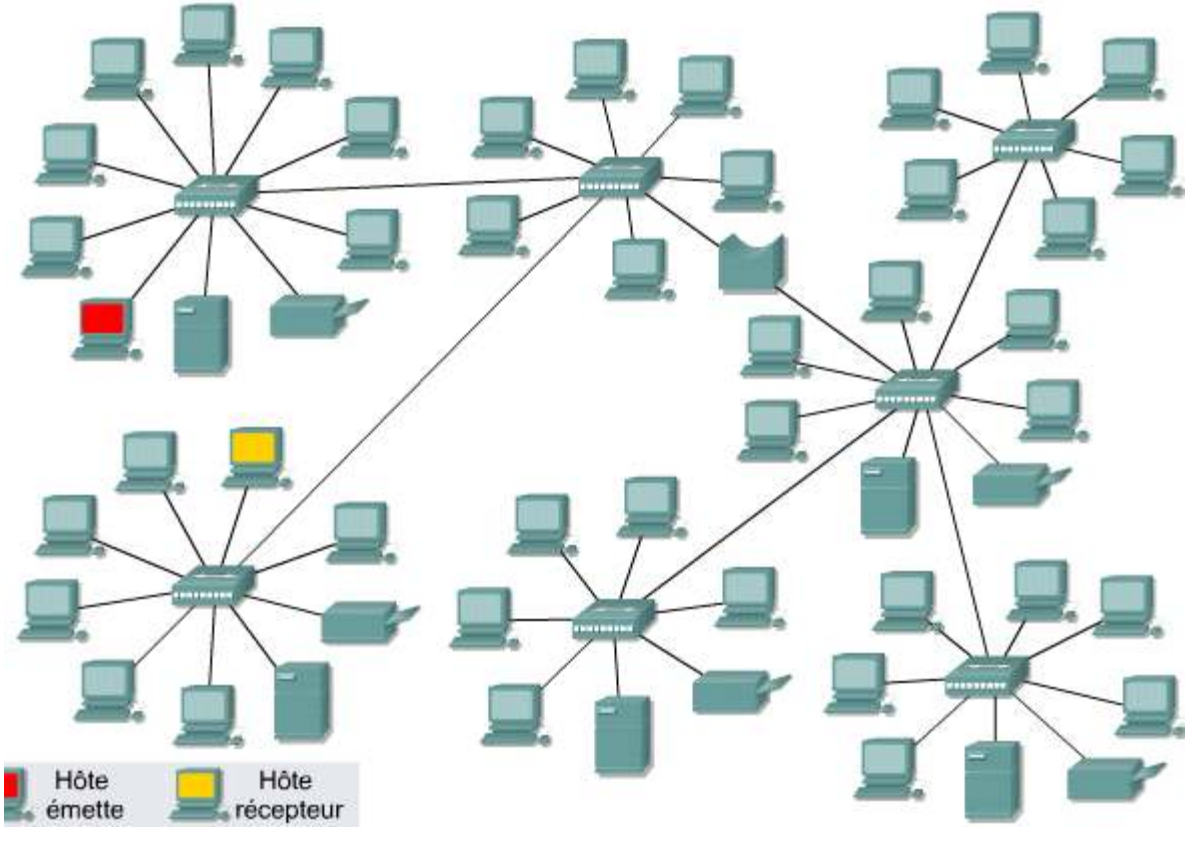


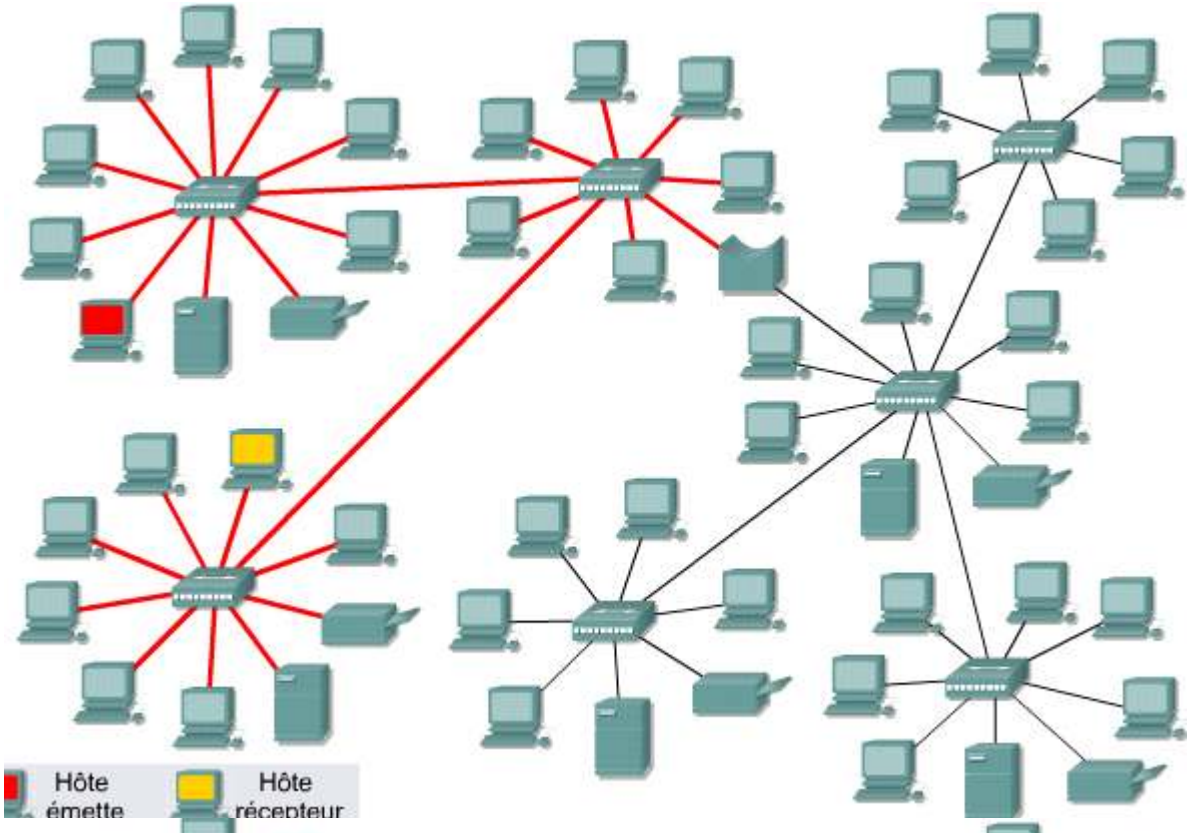
Fenêtre contextuelle (pop up)

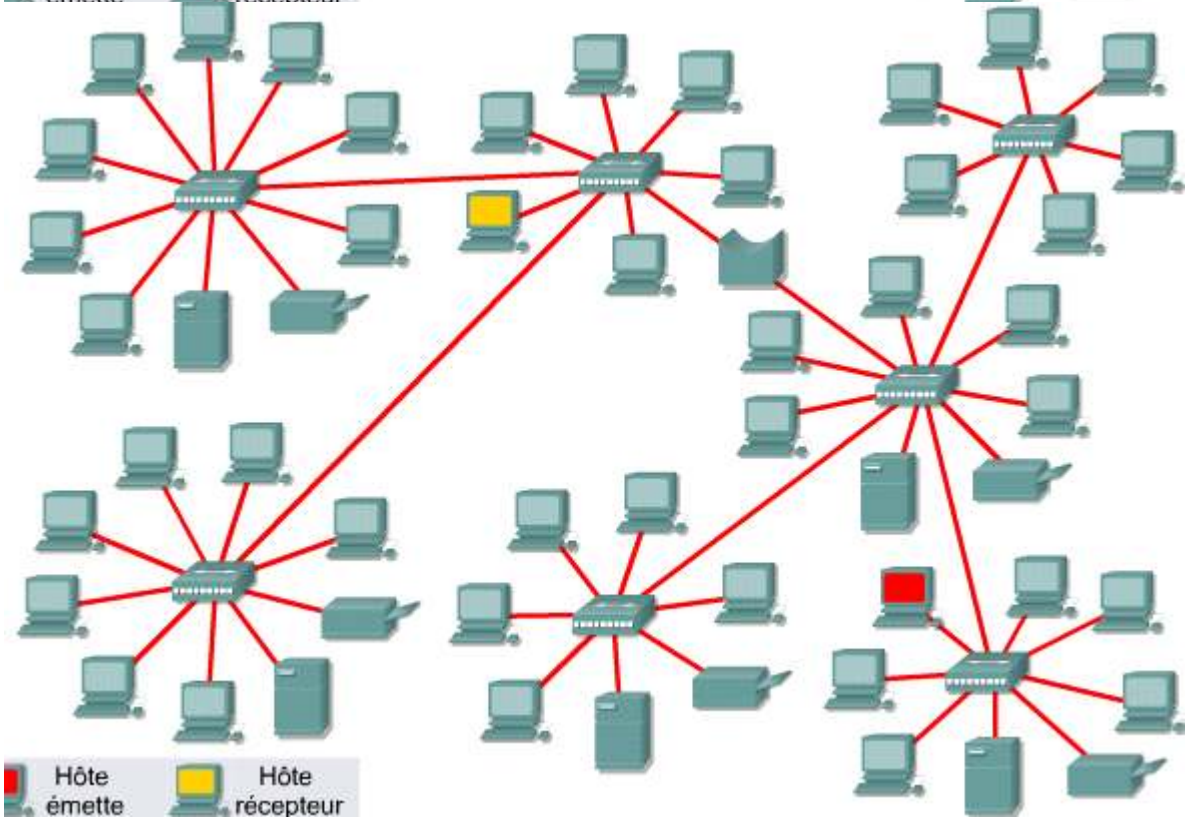
Ce réseau, composé de 43 hôtes, de 5 serveurs, de 5 imprimantes réseau et de 7 concentrateurs, constitue un domaine de collision/de broadcast unique. Lorsqu'un hôte ou un serveur effectue une transmission, tous les autres équipements la reçoivent. Plus important encore, lorsqu'un équipement du réseau envoie des données, aucun des autres équipements du réseau ne peut en envoyer simultanément.

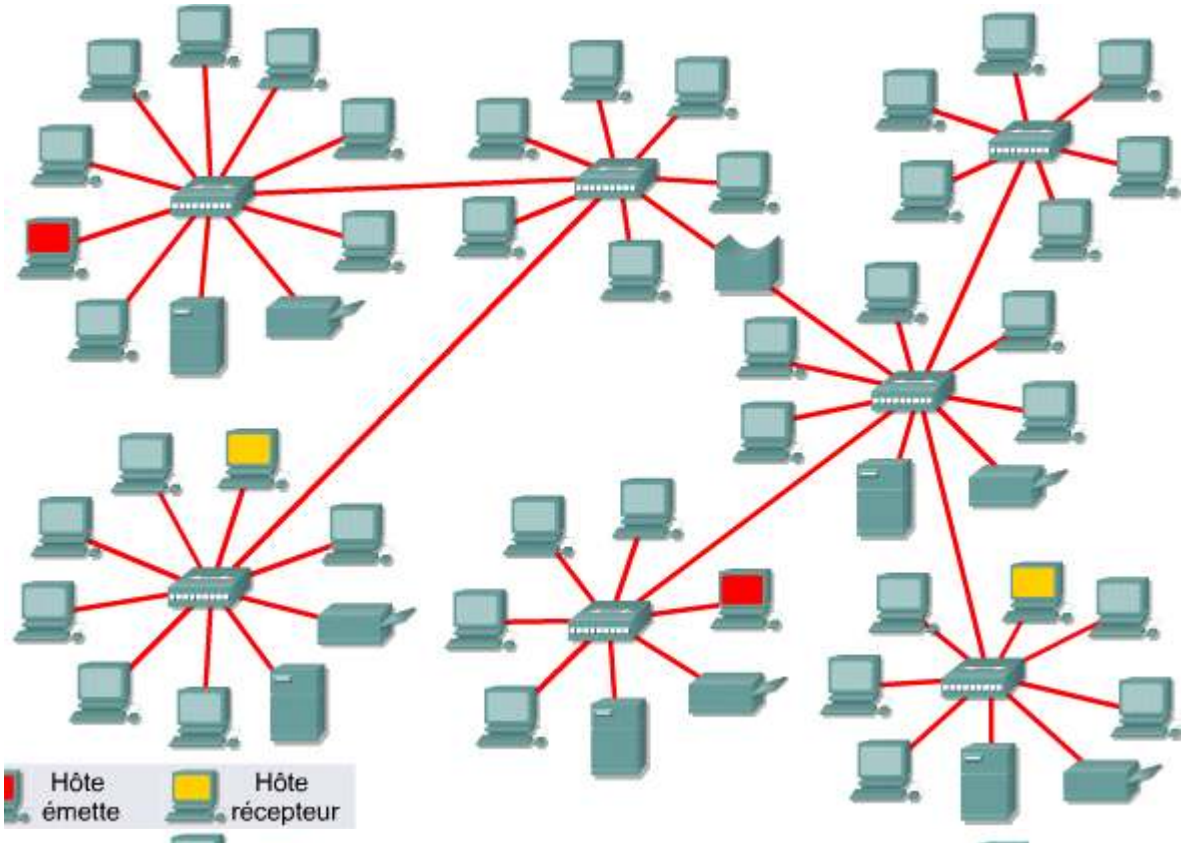

Hôte émette
Hôte récepteur

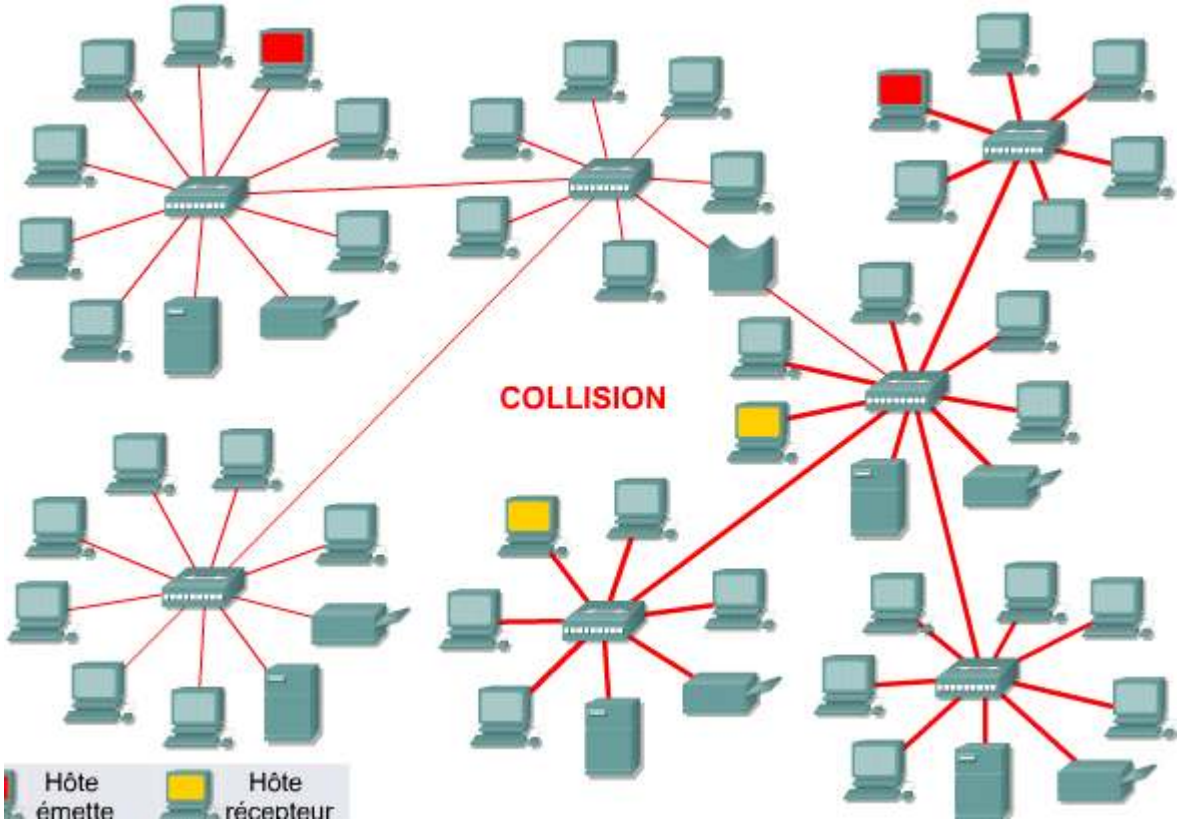

COLLISION
Hôte émette
Hôte récepteur


Hôte émette
Hôte récepteur


Hôte émette
Hôte récepteur


Hôte émette
Hôte récepteur


Hôte émette
Hôte récepteur


COLLISION
Hôte émette
Hôte récepteur

Moins il y a d'hôtes dans un domaine de collision, plus la disponibilité du média est élevée. Ce type de réseau fonctionne parfaitement si le trafic entre les segments reliés par des ponts n'est pas trop chargé. Sinon, l'équipement de couche 2 devient un goulot d'étranglement, ce qui ralentit la vitesse de communication.

Les équipements de couche 2 et 3 ne transmettent pas les collisions. Les équipements de couche 3 subdivisent les domaines de collision en domaines plus petits.

En outre, ils disposent d'autres fonctions. Ces dernières seront décrites dans la section relative aux domaines de broadcast.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux cerner le processus de segmentation du réseau.

La page suivante aborde la notion de broadcast.

Activité de média interactive

Complétez les zones vides: Segmentation

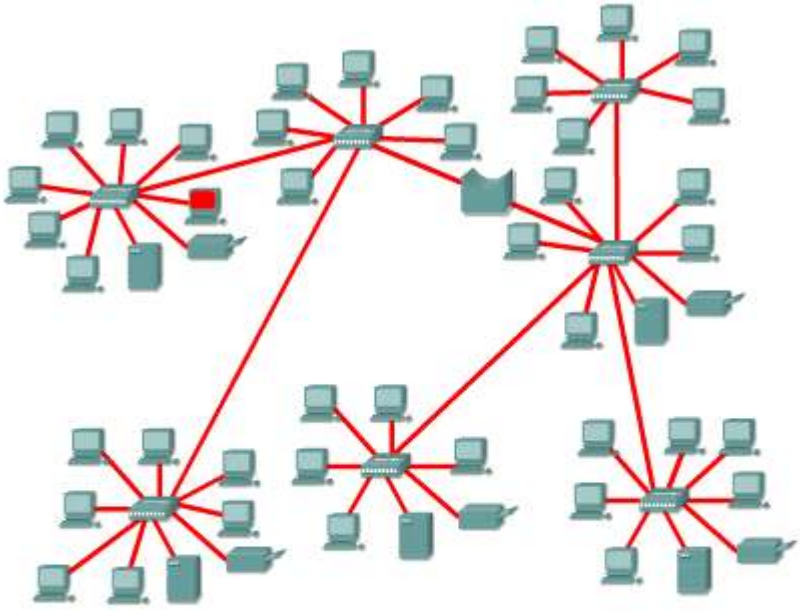
Après avoir complété cette activité, l'étudiant aura une meilleure compréhension de la segmentation réseau.

8.2 Domaines de collision et de broadcast

8.2.4 Broadcast au niveau de la couche 2

Cette page explique les modalités d'utilisation des broadcasts au niveau de la couche 2.

Pour communiquer avec tous les domaines de collision, les protocoles utilisent les trames de diffusion broadcast et multicast au niveau de la couche 2 du modèle OSI. [1]

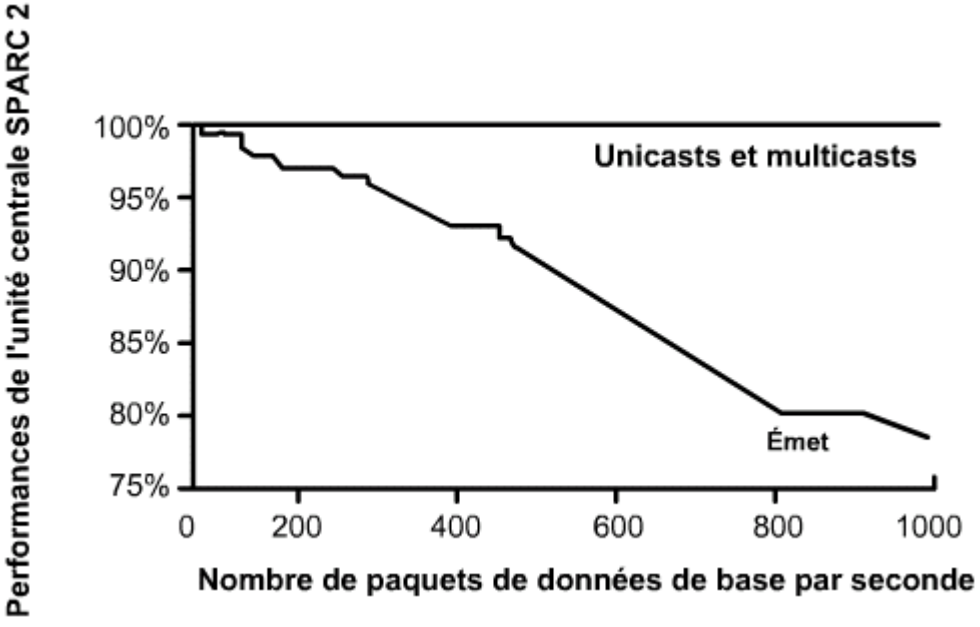


Un broadcast est récupéré par toutes les stations. Un broadcast traverse également tous les ponts, que l'hôte récepteur soit de l'autre côté du pont ou non. Cette caractéristique supprime les avantages d'une solution réseau avec pont.

Lorsqu'un nœud doit communiquer avec tous les hôtes du réseau, il envoie une trame de broadcast avec une adresse MAC de destination 0xFFFFFFFFFFFF. La carte réseau de chaque hôte doit alors envoyer une réponse à cette adresse.

Les équipements de couche 2 doivent diffuser la totalité du trafic de broadcasts et de multicast. L'accumulation du trafic de broadcasts et de multicast de chaque équipement du réseau s'appelle le rayonnement de diffusion (*broadcast radiation*). Il arrive alors que le réseau soit saturé au point que les données d'application ne disposent plus d'une bande passante suffisante. Lorsque cela se produit, il est impossible d'établir de nouvelles connexions, et certaines connexions en cours sont interrompues. Cette situation est connue sous le nom de tempête de broadcasts. Plus le réseau commuté prend de l'importance et plus le risque de tempête de broadcasts devient fort.

Une carte réseau dépend du processeur pour traiter chaque groupe de broadcasts ou de multicasts auquel elle appartient. Par conséquent, le rayonnement de diffusion influe sur les performances des hôtes du réseau. La figure 2



indique le résultat des tests effectués par Cisco concernant les effets du rayonnement de diffusion sur les performances du processeur Sun SPARCstation 2 doté d'une carte intégrée Ethernet classique. Les résultats démontrent clairement que les broadcasts diffusés sur le réseau peuvent entraîner l'arrêt de la station de travail IP. Des pics exceptionnels de broadcasts ont été observés pendant les tempêtes de broadcasts (milliers de broadcasts par seconde). Les tests effectués dans un environnement contrôlé avec plusieurs broadcasts et multicasts sur le réseau indiquent une diminution notable des performances du système avec moins de 100 broadcasts ou multicasts par seconde.

Un hôte ne gagne rien à traiter un broadcast qui ne correspond pas à la destination voulue. L'hôte n'est pas concerné par le service qui est annoncé. Un rayonnement de diffusion élevé peut dégrader les performances de l'hôte de manière significative. Les trois sources de broadcasts et de multicasts dans les réseaux IP sont les stations de travail, les routeurs et les applications multicast.

Les stations de travail diffusent une requête ARP (*Address Resolution Protocol*) chaque fois qu'elles doivent localiser une adresse MAC qui ne se trouve pas dans la table ARP. 3

Nombre d'hôtes	Pourcentage moyen de perte d'unité centrale par hôte
100	.14
1000	.96
10000	9.15

Bien que les valeurs indiquées dans la figure puissent paraître relativement faibles, elles représentent un réseau IP classique, relativement bien conçu. Lorsqu'un pic de broadcasts ou de multicasts se produit en raison d'une tempête, la diminution des performances du processeur peut être beaucoup plus importante que la normale. Les tempêtes de broadcasts peuvent provenir d'un équipement qui demande des informations à un réseau devenu trop important. Le nombre impressionnant de réponses envoyées à la requête d'origine empêche l'équipement de les traiter, ou la première requête déclenche des requêtes similaires sur les autres équipements, bloquant ainsi le trafic normal du réseau.

Par exemple, la commande **`telnet mumble.com`** traduit un nom en une adresse IP lorsque vous utilisez le système DNS. Une requête ARP est diffusée pour localiser l'adresse MAC. En général, les stations de travail IP

peuvent conserver de 10 à 100 adresses dans le cache ARP pendant environ 2 heures. Dans une station de travail standard, le débit du protocole ARP est d'environ 50 adresses toutes les 2 heures (soit 0,007 adresse par seconde). Par conséquent, 2 000 stations d'extrémité IP fourniront environ 14 adresses par seconde.

Les protocoles de routage qui sont configurés sur un réseau peuvent augmenter de manière significative le trafic de broadcasts. Certains administrateurs configurent la totalité des stations de travail de sorte qu'elles utilisent le protocole RIP (*Routing Information Protocol*) comme garantie d'accessibilité et de redondance. Toutes les 30 secondes, le protocole RIPv1 utilise les broadcasts pour transmettre la table de routage RIP complète vers d'autres routeurs RIP. Si 2 000 stations de travail sont configurées pour exécuter le protocole RIP, ces stations génèrent 3 333 broadcasts par seconde sachant qu'une moyenne de 50 paquets est requise pour transmettre la table de routage. La plupart des administrateurs réseau configurent le protocole RIP sur cinq à dix routeurs uniquement. Pour une table de routage comprenant 50 paquets, 10 routeurs RIP génèrent environ 16 broadcasts par seconde.

Les applications de multicast IP peuvent nuire aux performances des réseaux commutés personnalisés de grande taille. La diffusion multicast est un moyen efficace d'envoyer un flux de données multimédias à plusieurs utilisateurs d'un concentrateur à média partagé. Toutefois, ce mode de diffusion n'est pas adapté aux réseaux commutés non hiérarchiques. Une application vidéo peut générer un flux de données multicast de 7 Mo qui serait envoyé à chaque segment. Cela provoquerait de graves problèmes d'encombrement.

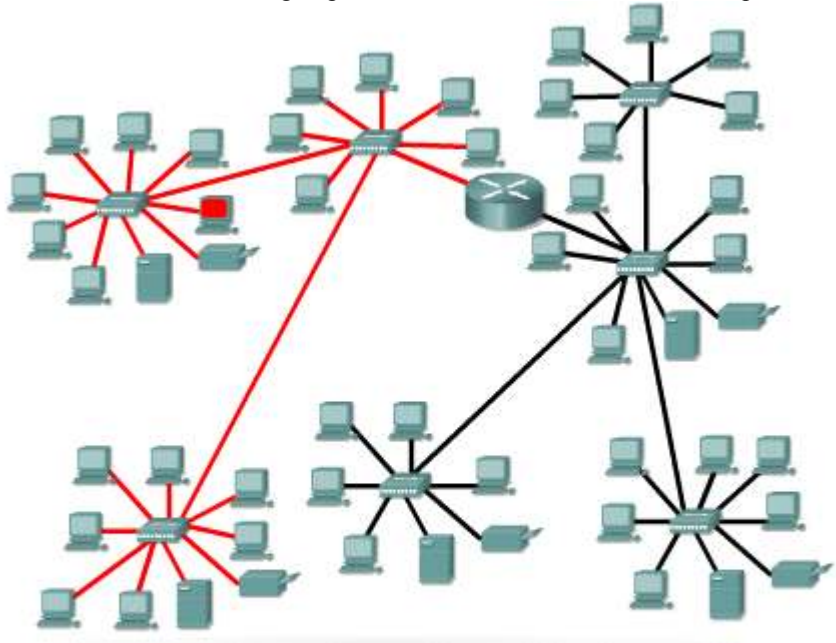
La page suivante décrit les domaines de broadcast.

8.2 Domaines de collision et de broadcast

8.2.5 Les domaines de broadcast

Cette page décrit les caractéristiques d'un domaine de broadcast.

Un domaine de broadcast est un groupe de domaines de collision connectés par des équipements de couche 2.



L'utilisation d'un routeur plutôt qu'une unité de pontage permet de contenir un broadcast de couche 2. Les équipements de couche 3 sont les seuls à contenir des broadcasts.

1

Lorsqu'un réseau LAN est subdivisé en plusieurs domaines de collision, chaque hôte du réseau peut accéder plus facilement au média. Les risques de collision sont réduits et la bande passante disponible pour chaque hôte est plus importante. Les broadcasts sont transmis par les équipements de couche 2. Un trop grand nombre de broadcasts peut nuire aux performances du réseau LAN tout entier. Les broadcasts doivent être contrôlés au niveau de la couche 3, car les équipements de couche 1 et 2 ne sont pas capables d'effectuer cette opération. Un domaine de broadcast comprend la totalité des domaines de collision qui traitent une même trame de broadcast. Ainsi, les nœuds appartenant au segment du réseau relié par un équipement de couche 3 font également partie du domaine de broadcast. Les domaines de broadcast sont contrôlés au niveau de la couche 3, car les routeurs n'acheminent pas les broadcasts. Les routeurs opèrent au niveau des couches 1, 2 et 3. À l'instar de tous les équipements de couche 1, les routeurs disposent d'une connexion physique et transmettent les données sur le média. En outre, les routeurs procèdent à l'encapsulation de couche 2 sur toutes les interfaces et effectuent les mêmes opérations que les autres équipements de couche 2. La couche 3 permet aux routeurs de segmenter les domaines de broadcast.

Pour qu'un paquet puisse être envoyé via un routeur, celui-ci doit déjà avoir été traité par un équipement de couche 2 et les informations relatives à la trame doivent avoir été éliminées. La transmission de couche 3 est fonction de l'adresse IP de destination et non de l'adresse MAC. Pour qu'un paquet soit envoyé, celui-ci doit contenir une adresse IP qui n'appartienne pas à la plage d'adresses affectées au réseau LAN et le routeur doit disposer de la destination du paquet dans sa table de routage.

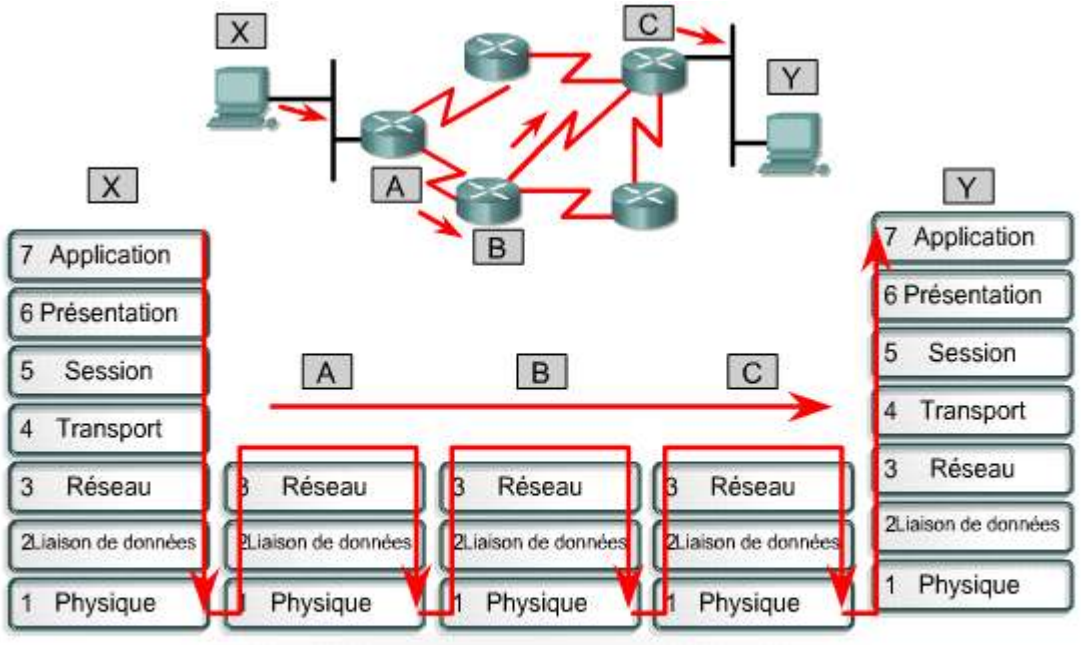
La page suivante traite du flux des données.

8.2 Domaines de collision et de broadcast

8.2.6 Présentation du flux des données

Cette page présente les flux de données.

Dans le contexte des domaines de collision et de broadcast, les flux de données sont principalement axés sur la propagation des trames de données dans un réseau. Cette notion décrit les mouvements de données dans les équipements de couche 1, 2 et 3, ainsi que la façon dont les données sont encapsulées pour être acheminées. N'oubliez pas que les données sont encapsulées à l'aide des adresses IP source et de destination au niveau de la couche réseau et des adresses MAC source et de destination au niveau de la couche liaison de données. 1



Le flux de données dans un réseau concerne les couches 1, 2 et 3 du modèle OSI. Il s'agit donc du trajet entre la transmission des données par l'hôte émetteur et leur arrivée au niveau de l'hôte récepteur.

Voici la règle expliquant la différence: un équipement de couche 1 transmettra toujours une trame, alors qu'un équipement de couche 2 essayera toujours de la transmettre. En d'autres mots, l'équipement de couche 2 transmet toujours les trames à moins qu'un événement ne l'en empêche. Un équipement de couche 3 ne transmet pas de trame à moins d'y être obligé. L'utilisation de cette règle permet d'identifier comment les données sont acheminées sur un réseau.

Les équipements de couche 1 n'effectuent pas de filtrage. Par conséquent, la totalité des données reçues est transmise au segment suivant. La trame est simplement régénérée et resynchronisée afin de retrouver sa qualité de transmission initiale. Tous les segments reliés par des équipements de couche 1 appartiennent au même domaine (collision et broadcast).

Les équipements de couche 2 filtrent les trames de données en fonction des adresses MAC de destination. Une trame est transmise s'il s'agit d'une adresse inconnue qui se trouve en dehors du domaine de collision. La trame est également transmise s'il s'agit d'une adresse de broadcast, de multicast ou d'unicast devant être acheminée en dehors du domaine de collision local. La non-transmission d'une trame se produit uniquement dans le cas où un équipement de couche 2 détecte que l'hôte émetteur et l'hôte récepteur se trouvent dans le même domaine de collision. Un équipement de couche 2, tel qu'un pont, crée plusieurs domaines de collision, mais ne gère qu'un seul domaine de broadcast.

Les équipements de couche 3 filtrent les paquets de données en fonction des adresses IP de destination. Un paquet sera transmis uniquement si son adresse IP de destination est en dehors du domaine de broadcast et que le routeur a identifié l'adresse à laquelle envoyer le paquet. Un équipement de couche 3 crée plusieurs domaines de collision et de broadcast.

Le flux des données transitant sur un réseau de routage IP implique le passage des données par des équipements de gestion du trafic au niveau des couches 1, 2 et 3 du modèle OSI. La couche 1 sert à la transmission des données sur le média physique, la couche 2 à la gestion du domaine de collision et la couche 3 à la gestion du domaine de broadcast.

La page suivante définit un segment de réseau.

8.2 Domaines de collision et de broadcast

8.2.7 Qu’est-ce qu’un segment de réseau?

Cette page explique ce qu'est un segment de réseau.

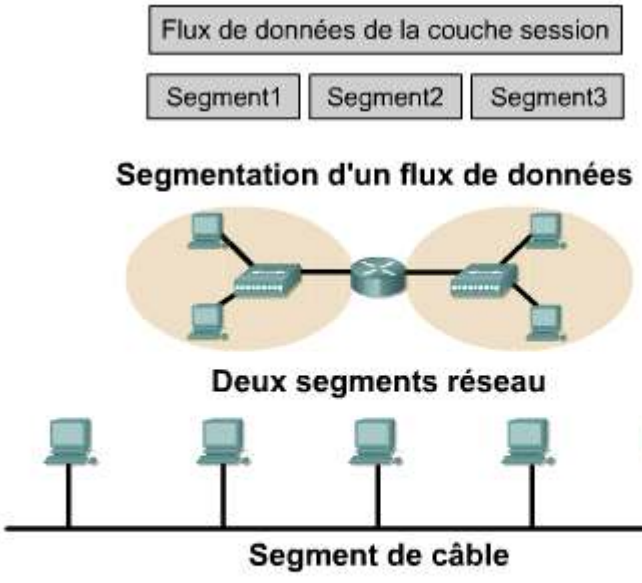
À l'instar de nombreux termes et acronymes, «segment» peut revêtir plusieurs sens. La définition du dictionnaire est la suivante:

- Partie détachée d'un ensemble
- L'une des parties qui résultent de la subdivision ou de la délimitation d'une entité en fonction de frontières naturelles ou pseudo-naturelles

Dans le domaine des échanges informatiques, la définition d'un segment est la suivante:

- Section d’un réseau reliée par des ponts, des routeurs ou des commutateurs.
- Dans un réseau local à topologie de bus, un segment est un circuit électrique continu souvent connecté à d’autres segments de même type par des répéteurs.
- C’est aussi un terme utilisé dans la spécification TCP pour décrire une unité d’information de la couche de transport. Les termes datagramme, trame, message et paquets sont aussi utilisés pour décrire des regroupements logiques de données au niveau de différentes couches du modèle de référence OSI dans divers cercles technologiques.

Pour que ce terme soit correctement défini, il doit être présenté dans son contexte. Si un segment est utilisé dans le contexte du protocole TCP, celui-ci est défini comme un élément de données séparé. Si un segment est utilisé dans le contexte d'un média réseau physique basé sur des routeurs, il est considéré comme étant l'une des parties, ou sections, du réseau complet. 1



Il existe différents types de segments dans un réseau. Selon le contexte d'une phrase, le terme " segment " peut donc désigner des éléments différents.

Les étudiants peuvent effectuer l'activité de média interactive pour identifier les trois types de segments possibles.

Cette page termine la leçon. La page suivante récapitule les principaux points évoqués au cours de ce module.

Activité de média interactive

Pointer-cliquer: Types de segments

À l'issue de cette activité, les étudiants auront appréhendé les diverses significations du terme segment.

Résumé

Cette page résume les sujets traités dans ce module.

La technologie Ethernet constitue un média partagé à bande de base, ce qui signifie qu'un seul nœud à la fois peut transmettre des données. L'augmentation du nombre de nœuds sur un segment unique entraîne une augmentation des besoins en bande passante, entraînant à son tour une augmentation des risques de collision. L'une des solutions consiste à fragmenter le segment réseau principal en plusieurs parties et à le subdiviser en domaines de collision distincts. Les ponts et les commutateurs ont été créés pour segmenter les réseaux en plusieurs domaines de collision.

Un pont crée une table de pontage à partir des adresses source des paquets qu'il traite. Chaque adresse est associée au port d'où provient la trame. Enfin, la table de pontage contient assez d'informations sur les adresses pour permettre au pont de transmettre une trame vers un port spécifique en fonction de son adresse de destination. C'est sur ce principe que le pont contrôle le trafic entre deux domaines de collision.

Les commutateurs fonctionnent de la même manière que les ponts, à une différence près : ils fournissent une connexion virtuelle entre les nœuds source et de destination, et non entre les domaines de collision source et de

destination. Chaque port crée son propre domaine de collision. Un commutateur crée et gère de façon dynamique une table de mémoire associative (CAM, *Content Addressable Memory*), qui contient toutes les informations MAC nécessaires à chaque port. En principe, la mémoire CAM effectue l'opération inverse des mémoires traditionnelles. Un contenu est fourni à la mémoire et l'adresse correspondante est récupérée.

Deux équipements réseau reliés par l'entremise d'un commutateur donnent naissance à deux domaines de collisions distincts. Ces petits segments physiques sont appelés des microsegments. Les microsegments qui sont connectés à l'aide de câbles à paires torsadées peuvent établir des communications en mode full duplex. Avec ce mode, lorsque vous utilisez des fils séparés pour la transmission et la réception entre deux hôtes, aucun confit d'accès entre routeurs ne se produit au niveau du média. Les domaines de collision n'existent plus.

Un délai de propagation existe lors de l'acheminement des signaux sur un support de transmission. En outre, le traitement des signaux par les équipements du réseau génère un retard supplémentaire, ou temps de latence.

La méthode de commutation d'une trame influe sur les phénomènes de latence et de fiabilité. Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue. Ce mode de commutation des paquets est appelé « Cut-through » et se caractérise par un temps de latence très faible. Toutefois, ce mode ne propose pas de contrôle d'erreurs. Néanmoins, il existe un commutateur pouvant recevoir la totalité de la trame avant de l'envoyer au port de destination. On parle alors de commutation « Store and Forward ». Le mode « Fragment Free » lit et vérifie les 64 premiers octets de la trame avant de l'envoyer au port de destination.

Les réseaux commutés possèdent très souvent des chemins redondants afin d'assurer une meilleure fiabilité et une meilleure tolérance aux pannes. Les commutateurs utilisent le protocole STP (*Spanning-Tree Protocol*) pour identifier et interrompre les chemins redondants sur le réseau. On obtient alors un chemin d'accès hiérarchique logique sans boucle.

L'utilisation des équipements de couche 2 pour subdiviser un réseau LAN en plusieurs domaines de collision permet d'augmenter la bande passante disponible pour chaque hôte. Toutefois, les équipements de couche 2 transmettent les broadcasts, tels que les requêtes ARP. Un équipement de couche 3 est requis pour contrôler les broadcasts et définir des domaines de broadcast.

Le flux des données transitant dans un réseau de routage IP implique le passage des données par des équipements de gestion du trafic au niveau des couches 1, 2 et 3 du modèle OSI. La couche 1 sert à la transmission des données sur le média physique, la couche 2 à la gestion du domaine de collision et la couche 3 à la gestion du domaine de broadcast.

Résumé

La compréhension des points clés suivants devrait être acquise :

- Modes de commutation classiques : • Store-and-forward • Cut-through • Fragment-free
- Le protocole Spanning-Tree permet de résoudre et d'éliminer les boucles d'un réseau.
- Les équipements de couche 1 ne segmentent pas les domaines de collision.
- Les équipements des couches 2 et 3 segmentent les domaines de collision.
- Les équipements des couches 1 et 2 ne bloquent pas les broadcasts.

9-Pile de protocoles TCP/IP et adressage IP

Vue d'ensemble

Internet a été créé dans le but de fournir un réseau de communication capable de fonctionner en cas de guerre. Malgré la considérable évolution de son objectif premier, il repose toujours sur la pile de protocoles TCP/IP. Le protocole TCP/IP s'avère parfaitement adapté aux exigences de robustesse et de décentralisation liées à Internet. En outre, la plupart des protocoles standard s'appuient sur le modèle TCP/IP à quatre couches.

Il est conseillé de disposer de connaissances sur les modèles de réseau OSI et TCP/IP. Chacun des modèles fait appel à sa propre structure pour décrire le mécanisme d'un réseau. Néanmoins, ils se recoupent beaucoup. Les administrateurs système doivent connaître ces modèles afin de saisir le mécanisme d'un réseau.

Pour échanger des données sur Internet, un équipement doit obligatoirement disposer d'un identificateur unique. Cet identificateur correspond à l'adresse IP, car les routeurs utilisent le protocole de couche 3 appelé «protocole IP» pour déterminer le meilleur chemin pour cet équipement. IPv4 est la version du protocole IP actuellement utilisée sur Internet. Celle-ci a été élaborée avant la forte augmentation du besoin en adresses. Face à la croissance démesurée d'Internet, le nombre d'adresses IP disponibles a dangereusement diminué. Pour répondre à cette pénurie d'adresses, des solutions ont été proposées : les sous-réseaux, le système NAT (*Network Address Translation*) et les adresses privées. Le protocole IPv6 apporte des améliorations à la version IPv4 et fournit un espace d'adressage beaucoup plus important. Cette version IPv6 permet aux administrateurs d'intégrer les méthodes disponibles dans la version IPv4, ou de les supprimer.

Pour se connecter à Internet, un ordinateur doit comporter une adresse MAC physique et une adresse IP unique. L'adresse IP unique est également appelée « adresse logique ». Il existe plusieurs façons d'attribuer une adresse IP à un équipement. Certains équipements possèdent toujours la même adresse statique, tandis que d'autres se voient attribuer une adresse différente à chaque connexion au réseau. L'allocation dynamique d'adresses IP peut s'effectuer de plusieurs manières différentes.

Pour que des données soient correctement acheminées d'un équipement à un autre, les problèmes liés, par exemple, à l'utilisation d'adresses en double doivent être résolus.

Ce module se rapporte à des objectifs spécifiques des examens de certification CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP afin de répondre aux exigences de • Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco	• Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • Mise en œuvre d'un LAN		• Évaluation du processus de communication TCP/IP et de ses protocoles associés • Description des communications réseau à l'aide des modèles en couche

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP pour la prise en charge de l'adressage par classe, sans classe et privé afin de répondre aux besoins de conception	• Mise en œuvre d'un LAN • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes		

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur • Détermination des adresses IP	• Attribution d'adresses IP • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des techniques d'adressage IP • Description de l'impact des protocoles associés à TCP/IP sur la communication des hôtes • Description du mode d'association entre une adresse IP et l'interface d'une unité, et de l'association entre les techniques d'adressage physique et d'adressage IP • Description des principes et de l'usage de la commutation de paquets utilisant le protocole IP (Internet Protocol)

À l'issue de ce module, les étudiants seront en mesure d'effectuer les actions suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
9.1	Présentation du protocole TCP/IP
9.2	Adresses Internet
9.3	Obtention d'une adresse IP

- Expliquer le principe d'Internet et l'adéquation du protocole TCP/IP avec celui-ci.
- Décrire les quatre couches du modèle TCP/IP.
- Spécifier les fonctions de chaque couche du modèle TCP/IP.
- Comparer les modèles OSI et TCP/IP.
- Présenter la fonction et la structure des adresses IP.
- Définir le rôle des sous-réseaux.
- Présenter les différences entre l'adressage privé et l'adressage public.
- Identifier la fonction des adresses IP réservées.
- Expliquer l'utilisation de l'adressage dynamique et statique d'un équipement.
- Définir le mécanisme des adresses dynamiques avec les protocoles RARP, BOOTP et DHCP.
- Utiliser le protocole ARP pour que l'adresse MAC envoie un paquet à un autre équipement.
- Appréhender les problèmes liés à l'adressage réseau.

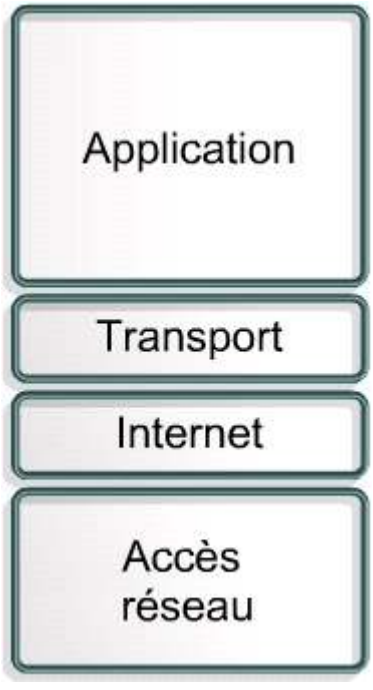
9.1 Présentation du protocole TCP/IP

9.1.1 Origine et évolution du protocole TCP/IP

Cette page traite de l'origine et de l'évolution du protocole TCP/IP.

Le ministère américain de la Défense (*DoD*) a développé le modèle de référence TCP/IP, car il avait besoin d'un réseau pouvant résister à toutes les situations. Imaginez en effet un monde quadrillé de connexions de toutes sortes : fils, micro-ondes, fibres optiques et liaisons satellites. Imaginez maintenant que des données doivent être transmises quel que soit l'état d'un nœud ou d'un réseau spécifique. Le ministère américain de la Défense nécessitait une transmission réseau fiable, pour toute destination des données et en toute circonstance. La création du modèle TCP/IP a contribué à la réalisation de ce projet. Depuis lors, le modèle TCP/IP s'est imposé comme la norme Internet.

Examinez les couches du modèle TCP/IP par rapport à l'objectif initial d'Internet afin d'éclaircir la situation. Les quatre couches du modèle TCP/IP sont les suivantes: la couche application, la couche transport, la couche Internet et la couche d'accès au réseau. 1



Certaines couches du modèle TCP/IP portent le même nom que celles du modèle OSI. Il est essentiel de ne pas confondre les fonctions des couches, car ces dernières jouent des rôles différents dans chaque modèle. La version actuelle du protocole TCP/IP a été normalisée en septembre 1981.

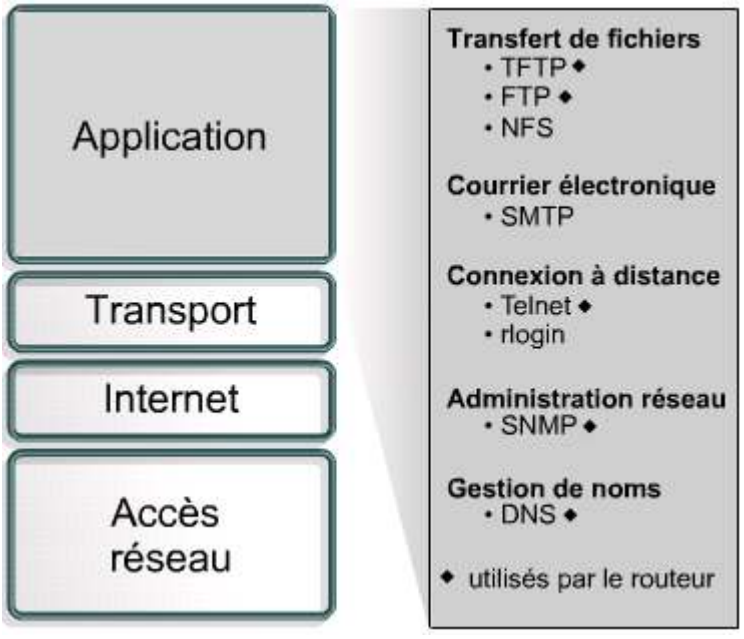
La page suivante traite de la couche application du protocole TCP/IP.

9.1 Présentation du protocole TCP/IP

9.1.2 La couche application

Cette page décrit les fonctions de la couche application du protocole TCP/IP.

La couche application gère les protocoles de niveau supérieur, les représentations, le code et le contrôle du dialogue. La pile de protocoles TCP/IP regroupe en une seule couche la totalité des aspects liés aux applications et vérifie que les données sont préparées de manière adéquate pour la couche suivante. Le protocole TCP/IP contient des spécifications relatives aux couches transport et Internet, notamment IP et TCP, et d'autres relatives aux applications courantes. Outre la prise en charge du transfert de fichiers, du courrier électronique et de la connexion à distance, le modèle TCP/IP possède des protocoles prenant en charge les services suivants: 1



- **Le protocole FTP *(File Transfer Protocol)*:** ce protocole est un service fiable orienté connexion qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. Il gère les transferts bidirectionnels des fichiers binaires et ASCII.
- **Le protocole TFTP *(Trivial File Transfer Protocol)*:** ce protocole est un service non orienté connexion qui utilise le protocole de datagramme utilisateur UDP (*User Datagram Protocol*). Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- **Le protocole NFS *(Network File System)*:** ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau.
- **Le protocole SMTP *(Simple Mail Transfer Protocol)*:** ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.
- **Telnet:** ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes. Un client Telnet est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.
- **Le protocole SNMP *(Simple Network Management Protocol)*:** ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.

- **Le protocole DNS *(Domain Name System)*:** ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les protocoles de la couche application.

La page suivante traite de la couche transport.

Activité de média interactive

Glisser-Positionner: La couche application

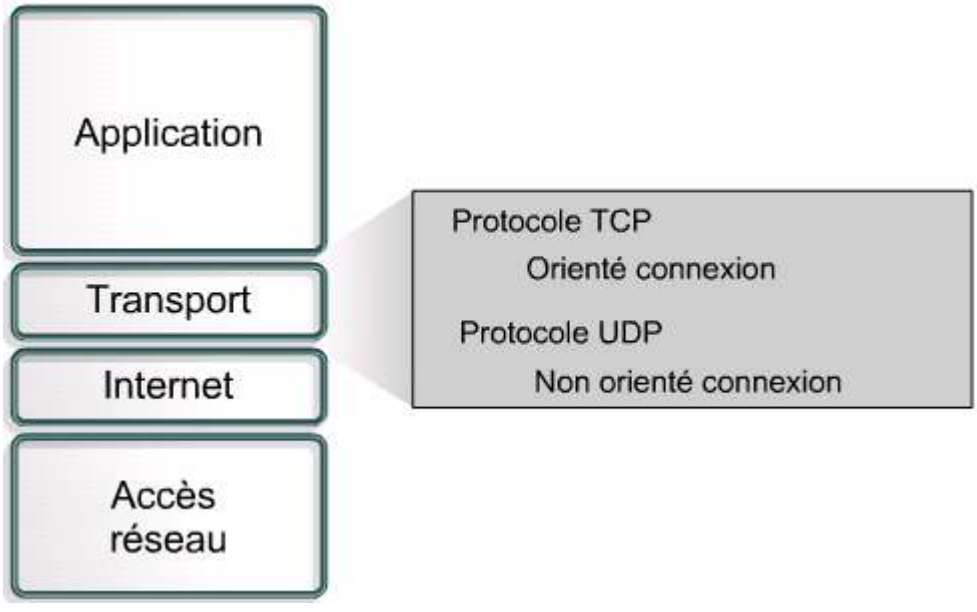
À l'issue de cette activité, les étudiants seront capables d'identifier les protocoles utilisés dans la couche application.

9.1 Présentation du protocole TCP/IP

9.1.3 La couche transport

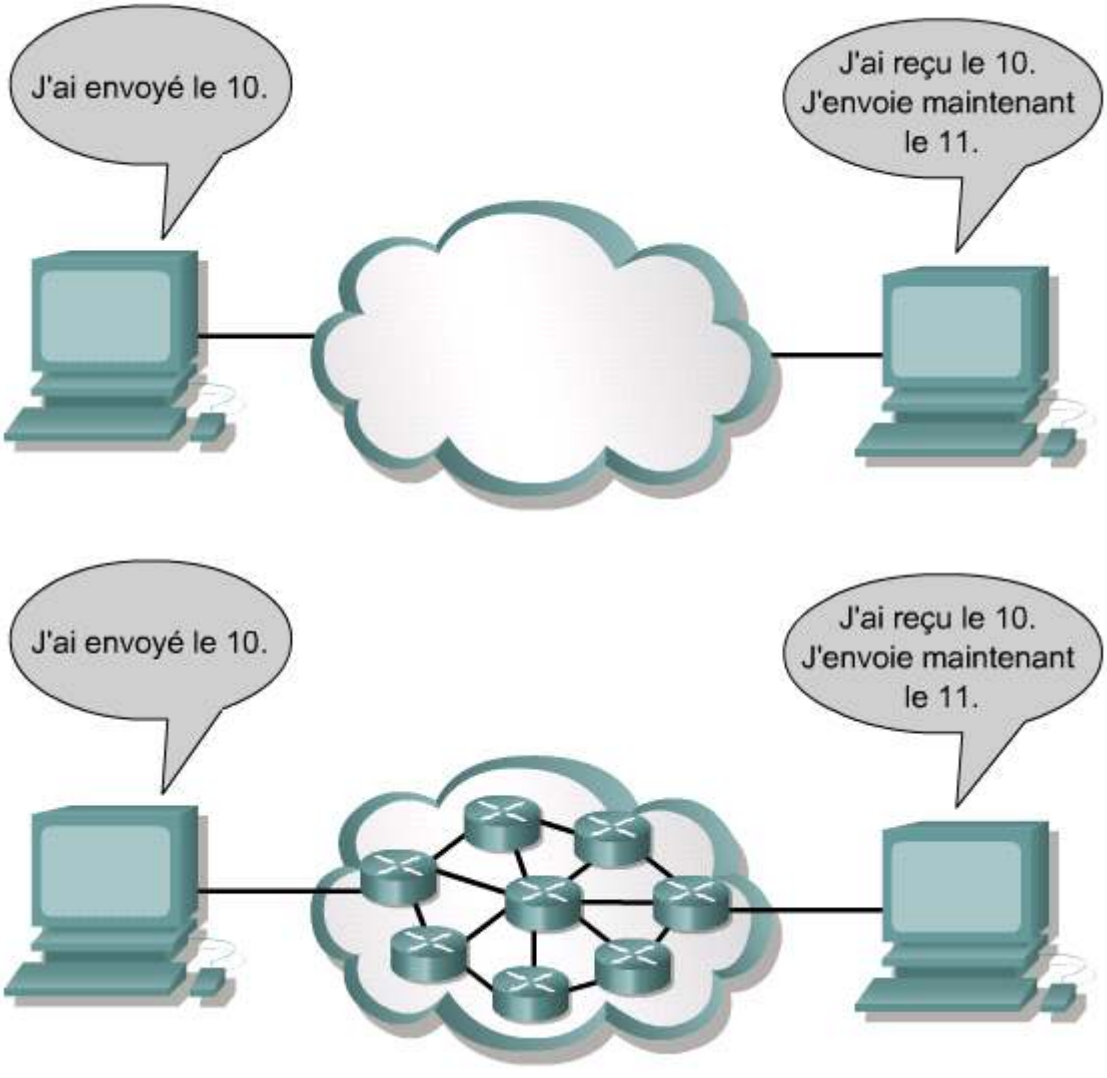
Cette page explique comment la couche transport offre des services de transport de l'hôte à la destination.

La couche transport fournit une connexion logique entre les hôtes source et de destination. 1



Les protocoles de transport segmentent et rassemblent les données envoyées par des applications de couche supérieure en un même flux de données, ou connexion logique, entre les deux points d'extrémité.

Internet est souvent représenté par un nuage. La couche transport envoie des paquets de données d'une source à une destination à travers ce nuage. 2 3



Le rôle principal de la couche transport est d'assurer une fiabilité et un contrôle de bout en bout lors du transfert des données à travers ce nuage. Les fenêtres glissantes, les numéros de séquençage et les accusés de réception permettent d'obtenir ce résultat. La couche transport définit également une connectivité de bout en bout entre les applications hôtes. Les protocoles de la couche transport incluent les protocoles TCP et UDP.

Le rôle des protocoles TCP et UDP est le suivant:

- Segmenter les données d'application de couche supérieure.
- Envoyer des segments d'un équipement à un autre.

Le rôle du protocole TCP est le suivant:

- Etablir une connexion de bout en bout.
- Assurer le contrôle de flux à l'aide des fenêtres glissantes.
- Assurer la fiabilité du réseau à l'aide des numéros de séquençage et des accusés de réception.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les protocoles de la couche transport.

La page suivante traite de la couche Internet.

Activité de média interactive

Case à cocher: La couche transport

À l'issue de cette activité, les étudiants seront capables d'identifier les protocoles utilisés dans la couche transport.

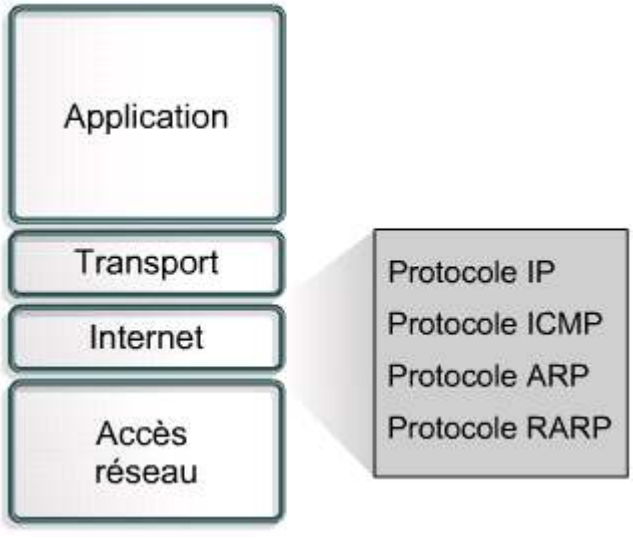
9.1 Présentation du protocole TCP/IP

9.1.4 La couche Internet

Cette page décrit les fonctions de la couche Internet du protocole TCP/IP.

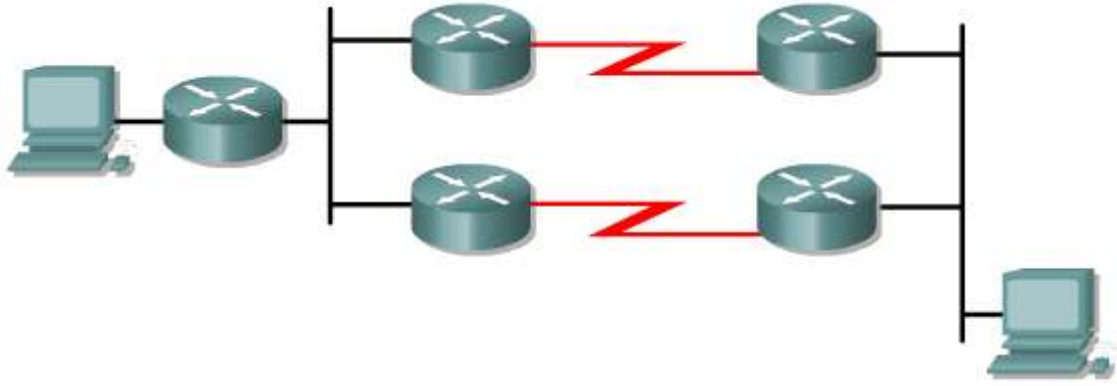
Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Le principal protocole de cette couche est le protocole IP. La détermination du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

Les protocoles ci-dessous s'exécutent au niveau de la couche Internet du protocole TCP/IP: 1

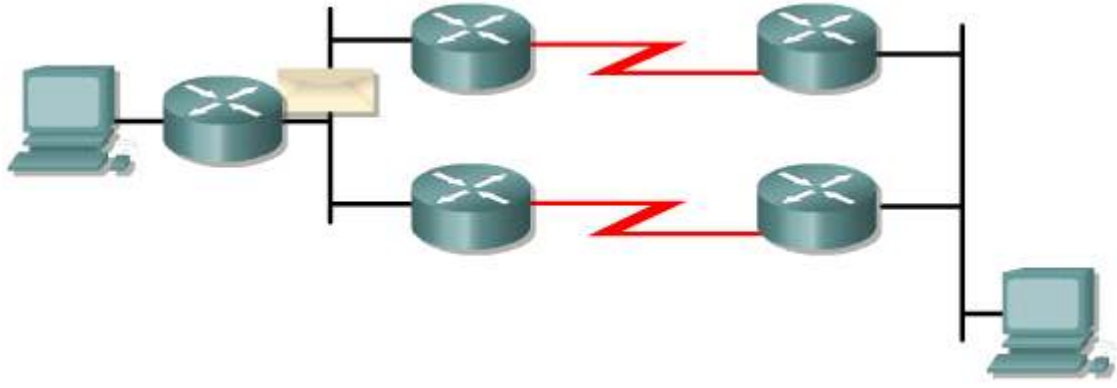


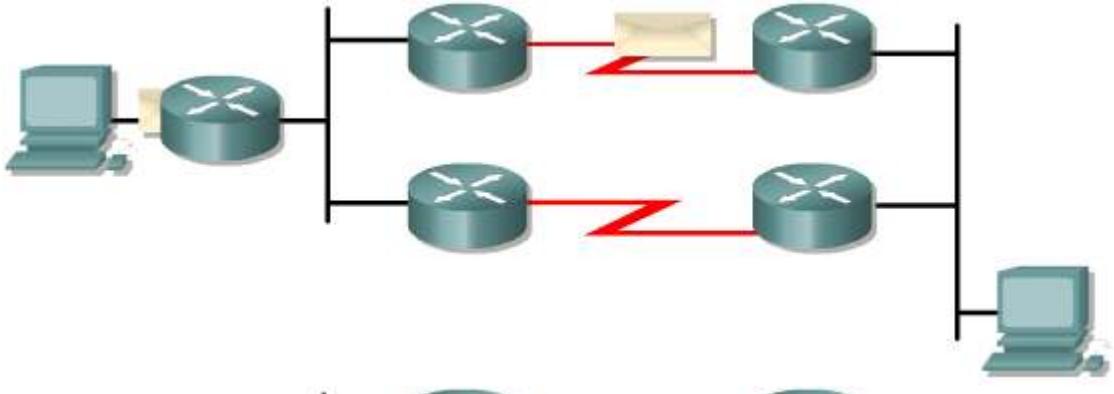
- Le protocole IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion. Il ne se préoccupe pas du contenu des paquets, mais il recherche un chemin pour les acheminer à destination.
- Le protocole ICMP (*Internet Control Message Protocol*) offre des fonctions de messagerie et de contrôle.
- Le protocole ARP (*Address Resolution Protocol*) détermine les adresses de la couche liaison de données ou les adresses MAC pour les adresses IP connues.
- Le protocole RARP (*Reverse Address Resolution Protocol*) détermine l'adresse IP pour une adresse MAC connue.

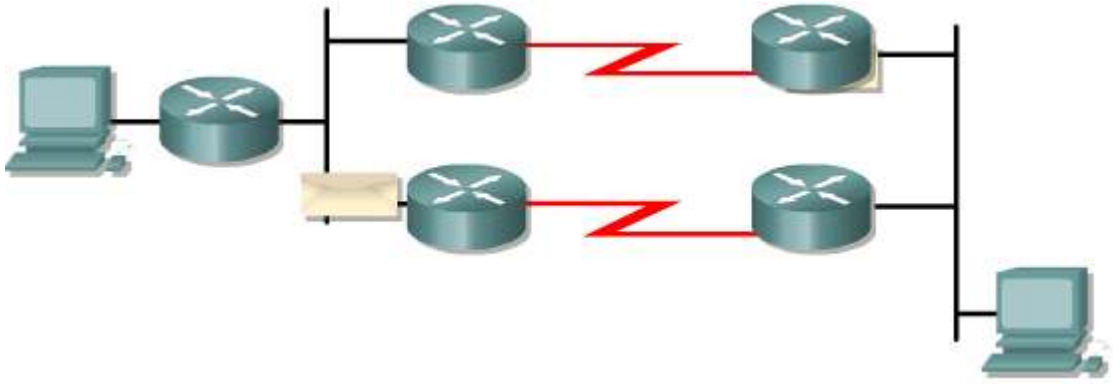
Le protocole IP effectue les opérations suivantes: 2

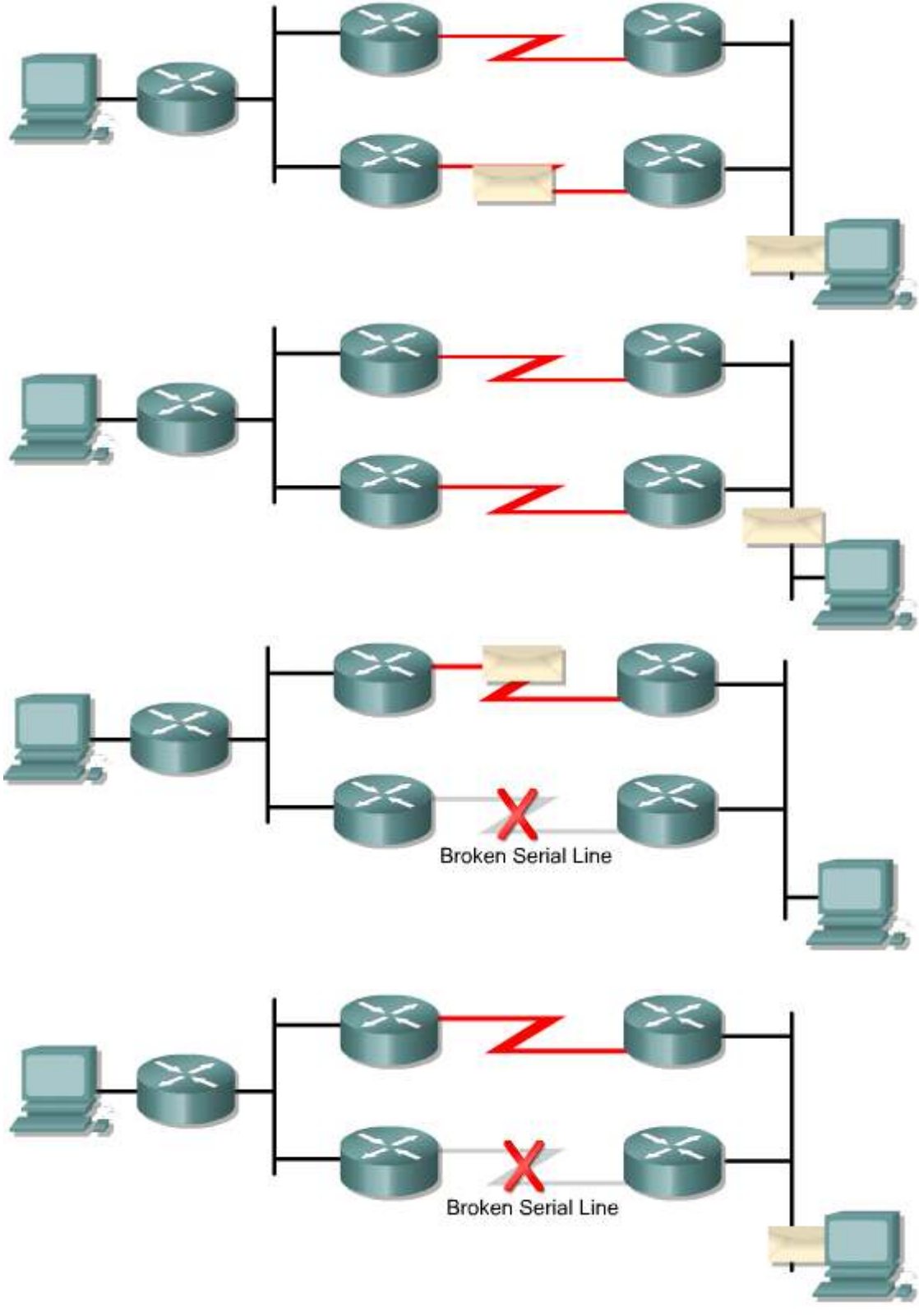


Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau.









- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

Le protocole IP est parfois qualifié de protocole non fiable. Cela ne signifie pas qu'il n'envoie pas correctement les données sur le réseau, mais qu'il n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction. Ces fonctions sont disponibles uniquement dans les protocoles de couche supérieure des couches application ou transport.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les protocoles de la couche Internet.

La page suivante traite de la couche d'accès au réseau.

Activité de média interactive

Glisser-Positionner: La couche Internet

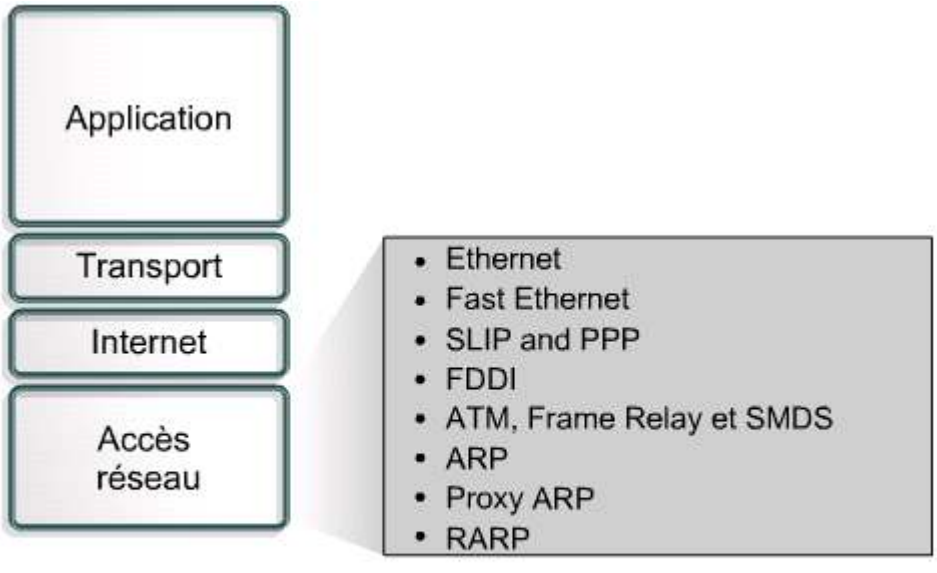
À l'issue de cette activité, les étudiants seront capables d'identifier les protocoles utilisés dans la couche Internet.

9.1 Présentation du protocole TCP/IP

9.1.5 La couche d'accès au réseau

Cette page décrit la couche d'accès au réseau du protocole ///TCP/IP, également connue sous le nom de couche hôte-réseau.

La couche d'accès au réseau permet à un paquet IP d'établir une liaison physique avec un média réseau. Cela comprend les détails sur les technologies LAN et WAN, ainsi que toutes les informations contenues dans les couches physique et liaison de données du modèle OSI. 1



Les protocoles ARP et RARP se situent au niveau des couches d'accès réseau et Internet.

Les pilotes d'application, les cartes modem et les autres équipements s'exécutent au niveau de la couche d'accès au réseau. Cette dernière définit les procédures utilisées pour communiquer avec le matériel réseau et accéder au média de transmission. Les protocoles de modem, à savoir les protocoles SLIP (*Serial Line Internet Protocol*) et PPP (*Point-to-Point Protocol*) sont utilisés pour accéder au réseau par modem. Plusieurs protocoles sont nécessaires pour déterminer les caractéristiques matérielles, logicielles et de transmission au niveau de cette couche. Cela peut entraîner une certaine confusion dans l'esprit des utilisateurs. La plupart des protocoles facilement reconnaissables s'exécutent au niveau des couches Internet et transport du protocole TCP/IP.

En outre, les protocoles de la couche d'accès au réseau mappent les adresses IP avec les adresses matérielles physiques et encapsulent les paquets IP dans des trames. La couche d'accès au réseau définit la connexion au média physique en fonction de l'interface réseau et du type de matériel utilisés.

Voici un exemple de configuration de la couche d'accès au réseau faisant appel à une installation système Windows et à une carte réseau tierce. Certaines versions de Windows détectent automatiquement la carte réseau et installent ensuite les pilotes appropriés. Avec des versions plus anciennes de Windows, l'utilisateur doit indiquer le pilote de la carte réseau. Les fabricants de cartes réseau fournissent ces pilotes sur des disques ou des CD-ROM.

Les étudiants peuvent effectuer l'activité de média interactive pour se familiariser avec les protocoles de la couche d'accès au réseau.

La page suivante présente les similitudes et les différences entre le modèle TCP/IP et le modèle de référence OSI.

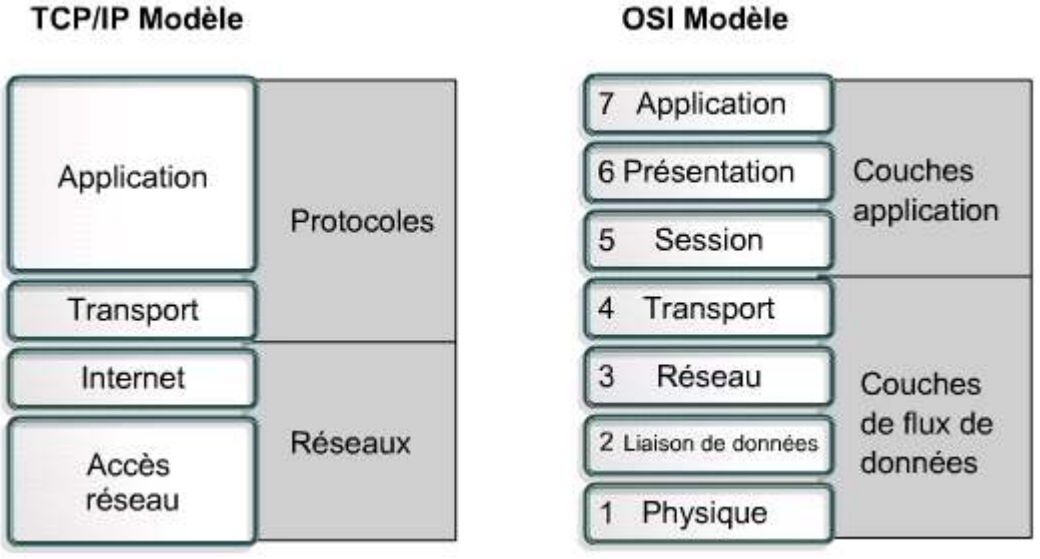


Activité de média interactive

Glisser-Positionner: La couche d’accès au réseau

À l'issue de cette activité, les étudiants seront capables d’identifier les protocoles utilisés dans la couche d'accès au réseau.

Dans cette page, le modèle OSI est mis en parallèle avec le modèle TCP/IP. 1



Les modèles OSI et TCP/IP présentent un grand nombre de similitudes:

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services différents.
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux s'appuient sur un réseau à commutation de paquets, et non sur un réseau à commutation de circuits.
- Les professionnels des réseaux doivent connaître les deux modèles.

Ils présentent également quelques différences:

- TCP/IP intègre les couches application, présentation et session du modèle OSI dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Lorsque la couche transport du protocole TCP/IP utilise le protocole UDP, la transmission des paquets n'est pas fiable tandis qu'elle est toujours fiable avec la couche transport du modèle OSI.

Les protocoles TCP/IP constituent la norme à partir de laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles. En règle générale, le modèle OSI ne permet pas de créer des réseaux. Il est utilisé pour aider les étudiants à comprendre le processus de communication.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux appréhender les différences entre les modèles de référence OSI et TCP/IP.

La page suivante examine l'architecture de base d'Internet.

Activité de média interactive

Glisser-Positionner: Comparaison des modèles OSI et TCP/IP

À l'issue de cette activité, les étudiants seront capables d'identifier les différences entre les modèles OSI et TCP/IP.

9.1 Présentation du protocole TCP/IP

9.1.7 L'architecture d'Internet

Cette page décrit l'architecture de base d'Internet.

Internet permet d'envoyer des données de façon quasi instantanée à partir de n'importe quel point du globe, et ce à tout moment.

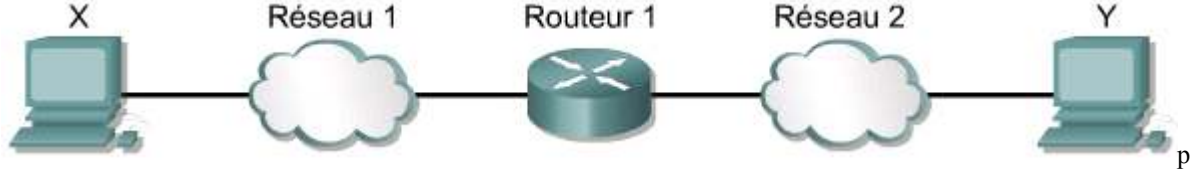
On appelle LAN les réseaux qui desservent une zone géographique limitée. Cependant, les LAN ne sont pas très évolutifs. Malgré les progrès techniques réalisés pour accélérer les communications, grâce notamment au réseau optique Metro et aux réseaux Gigabit et 10-Gigabit Ethernet, la distance reste un problème.

Afin d'obtenir une vue d'ensemble de l'architecture d'Internet, les étudiants analyseront les communications entre les ordinateurs source et de destination (ou les ordinateurs intermédiaires) au niveau de la couche application. Des instances identiques d'une application peuvent être installées sur tous les ordinateurs d'un réseau afin de faciliter l'acheminement des messages. Toutefois, ce système n'est pas très évolutif. Pour chaque nouveau logiciel, une nouvelle application doit alors être installée sur l'ensemble des ordinateurs du réseau et le logiciel doit être modifié afin d'éviter tout problème matériel. La défaillance d'un ordinateur intermédiaire ou d'une application installée sur un ordinateur pourrait interrompre la transmission des messages.

Internet fait appel au principe d'interconnexion de la couche réseau. L'objectif est de développer les fonctionnalités du réseau dans des modules séparés. Cela permet d'utiliser différentes technologies LAN pour les couches 1 et 2 du modèle OSI et différentes applications pour les couches 5, 6 et 7. Le modèle OSI offre un système dans lequel les caractéristiques des couches supérieures et inférieures sont indépendantes. Dès lors, les équipements de réseau intermédiaires auront la permission de relayer le trafic sans avoir de détails sur le LAN.

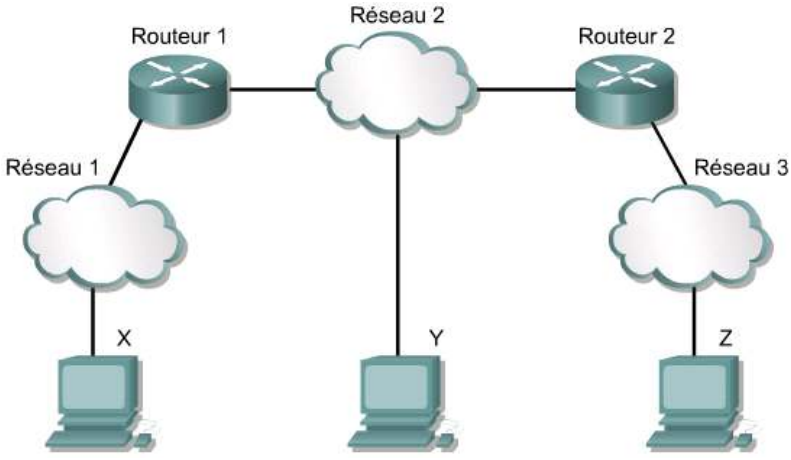
Ce qui nous amène au concept d'interréseaux, ou de réseaux composés de plusieurs réseaux. Un réseau qui comprend plusieurs réseaux s'appelle un interréseau. Le réseau sur lequel le Web (www) s'exécute s'appelle Internet. Les interréseaux doivent être modulables en fonction du nombre de réseaux et d'ordinateurs qui leur sont associés. En outre, les interréseaux doivent être capables de gérer l'acheminement des données sur de longues distances. Un interréseau doit être relativement flexible pour pouvoir assimiler les continuelles évolutions technologiques. Il doit être capable de s'adapter aux conditions dynamiques du réseau. Par ailleurs, les interréseaux doivent se révéler économiques. Ils doivent être conçus de manière à autoriser tout utilisateur à envoyer des données vers n'importe quelle destination, et ce à tout moment.

La figure 1



présente brièvement la connexion d'un réseau physique à un autre par l'intermédiaire d'un ordinateur spécifique appelé «routeur». Ces réseaux sont directement connectés au routeur. Les routeurs servent à prendre les décisions d'acheminement nécessaires à la communication entre deux réseaux. Plusieurs routeurs sont requis pour traiter un volume important de transmissions sur le réseau.

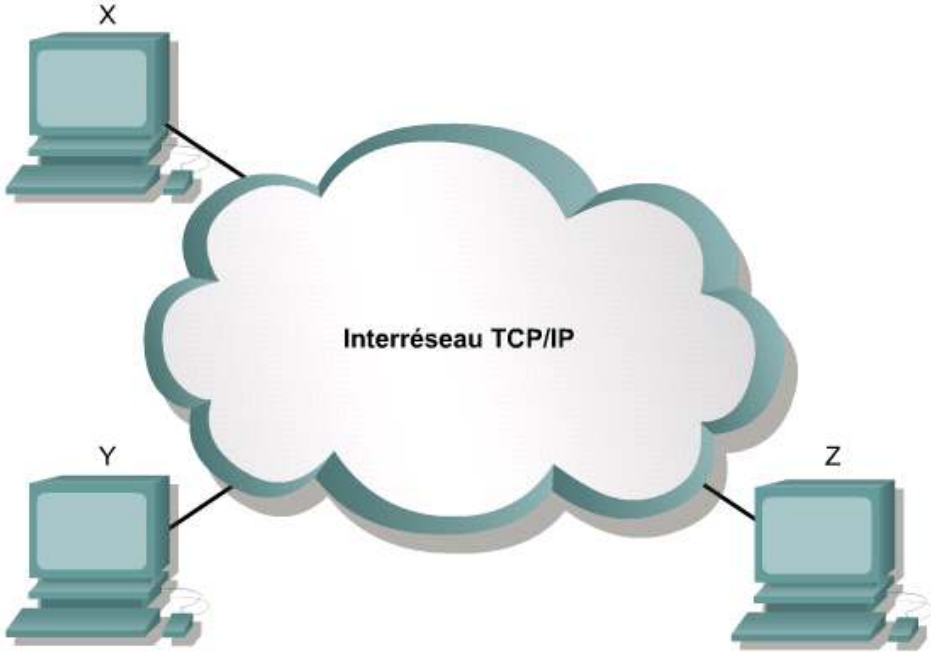
La figure 2



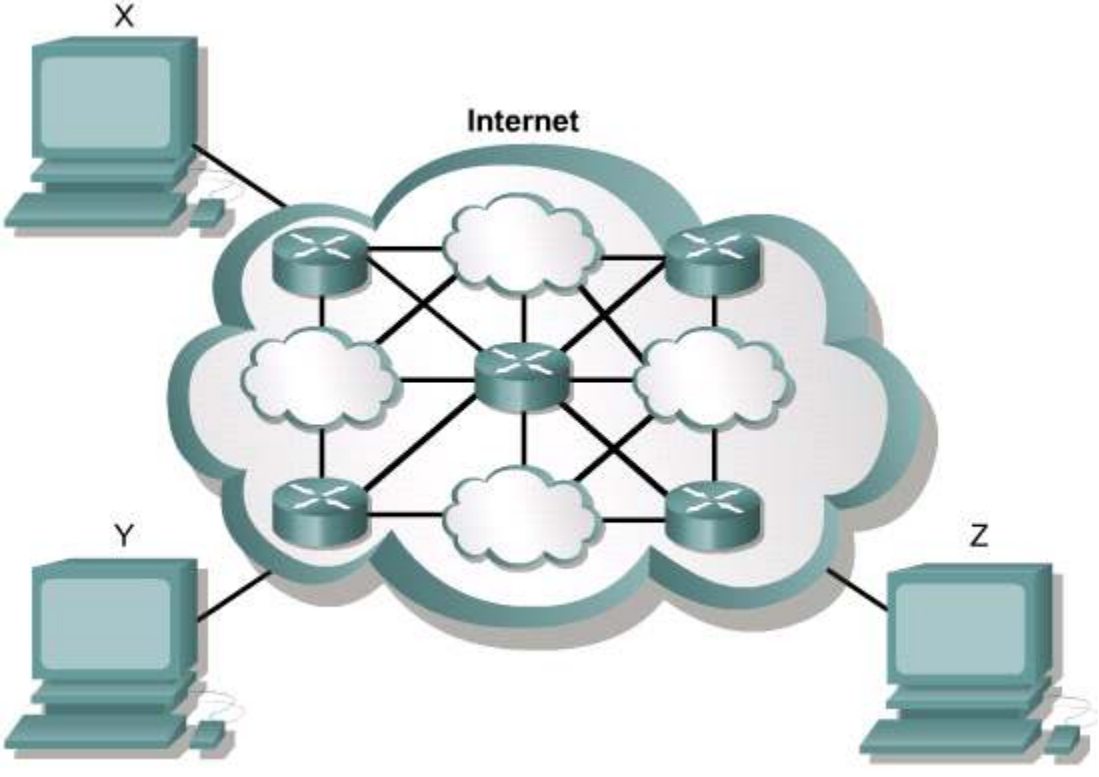
illustre trois réseaux physiques connectés par l'intermédiaire de deux routeurs. Ceux-ci prennent des décisions complexes afin de permettre aux utilisateurs de tous les réseaux de communiquer avec chacun d'entre eux. Les réseaux ne sont pas tous directement connectés entre eux. Par conséquent, les routeurs doivent définir une méthode pour gérer cette situation.

L'une des solutions consiste pour le routeur à établir une liste répertoriant tous les ordinateurs et leur chemin d'accès. Le routeur sélectionne ensuite la méthode d'envoi des paquets de données en fonction de cette table de référence. Les paquets sont alors envoyés en fonction de l'adresse IP de l'ordinateur de destination. Néanmoins, plus le nombre d'utilisateurs connectés au réseau augmente, plus cette solution s'avère compliquée. La notion d'évolutivité apparaît lorsque le routeur détient une liste de tous les réseaux, mais qu'il laisse la responsabilité de l'acheminement local aux réseaux physiques locaux. Dans ce cas, les routeurs transmettent les messages à d'autres routeurs. Chaque routeur partage des informations relatives à son réseau connecté.

La figure 3



présente la transparence du système requise par les utilisateurs. Néanmoins, les structures physiques et logiques qui composent le nuage Internet peuvent se révéler particulièrement complexes, comme l'illustre la figure 4



.

Internet a évolué rapidement, acceptant de plus en plus d'utilisateurs. Sa capacité d'évolution (plus de 90 000 routes principales et 300 000 000 utilisateurs finaux) traduit l'efficacité de son architecture.

Deux ordinateurs placés à deux endroits différents de la planète peuvent communiquer de façon fiable si tant est qu'ils respectent certaines exigences en matière de protocole et de configuration matérielle et logicielle. Internet a été rendu possible grâce à la normalisation des techniques de transmission des données sur les réseaux.

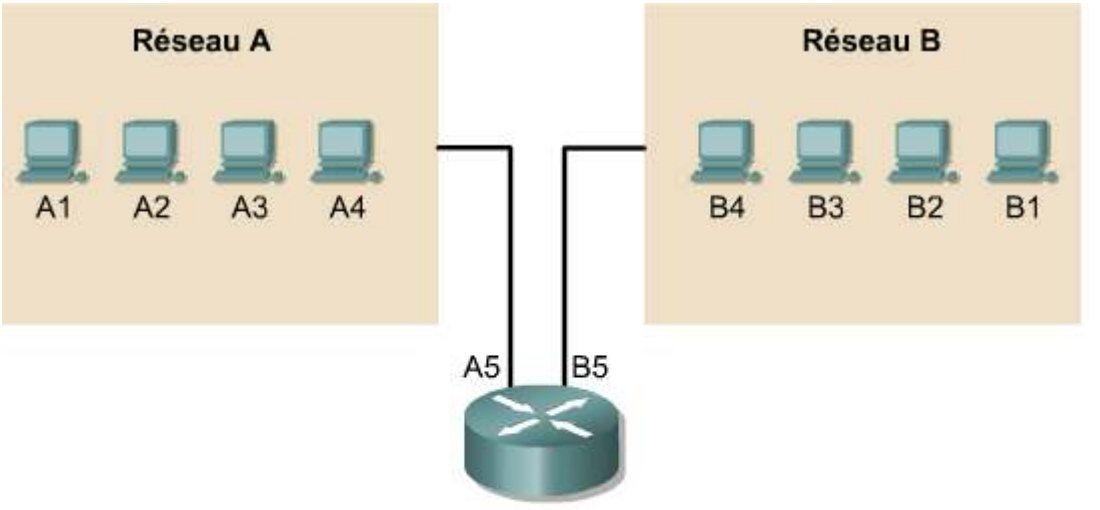
Cette page termine la leçon. La leçon suivante aborde la question de l'adressage Internet. La première page traite de l'adressage IP.

9.2 Les adresses Internet

9.2.1 L'adressage IP

Cette page décrit l'adressage IP.

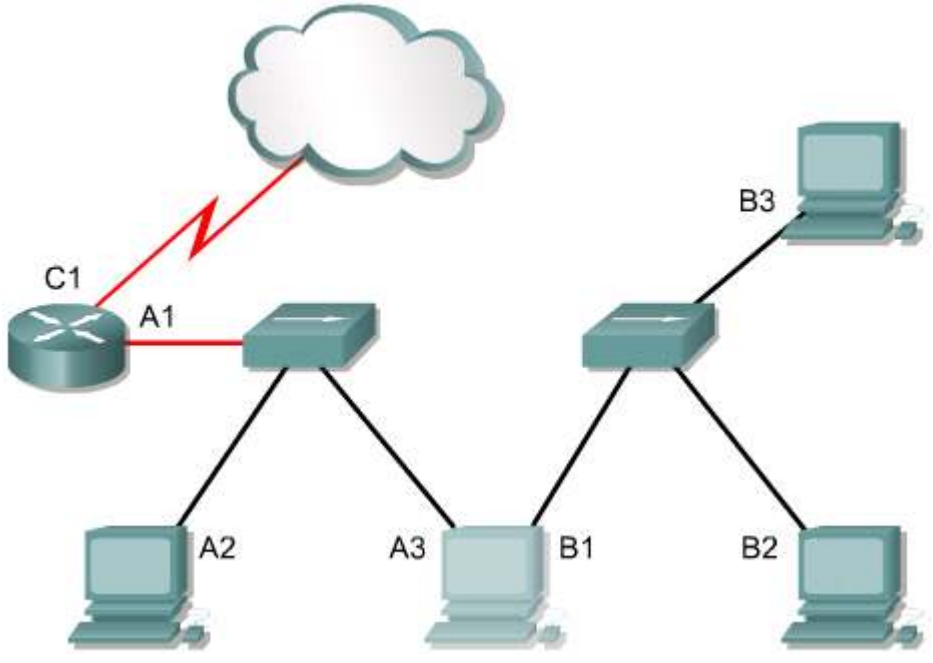
Lorsque deux systèmes veulent échanger des données, chacun d'eux doit pouvoir identifier et localiser l'autre. Les adresses indiquées dans la figure 1



Ces adresses ne correspondent pas à des adresses réseau réelles, mais elles illustrent le concept du regroupement d'adresses. Dans ce concept, les lettres A ou B identifient le réseau, et la séquence de nombres désigne l'hôte correspondant. La combinaison d'une lettre (adresse réseau) et d'un numéro (adresse hôte) crée une adresse unique pour chaque unité du réseau.

ne correspondent pas à des adresses réseau réelles, mais elles illustrent le concept du regroupement d'adresses.

Un ordinateur peut être connecté à plusieurs réseaux. 2

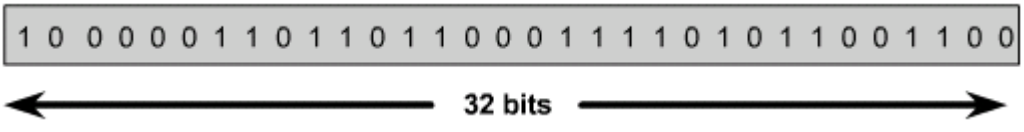


Fenêtre contextuelle (pop up)

Voici l'exemple d'un ordinateur connecté à deux réseaux différents. Pour cela, il dispose de deux cartes réseau. Il est alors désigné sous le nom d'unité à liaison double. Il est important de retenir que les deux interfaces de l'ordinateur se trouvant sur des réseaux totalement différents, elles disposent chacune d'un identificateur réseau distinct pour l'adresse. De plus, l'ordinateur ne transfère pas de données, à moins qu'il n'ait été configuré pour cette action, car il a simplement accès aux deux réseaux.

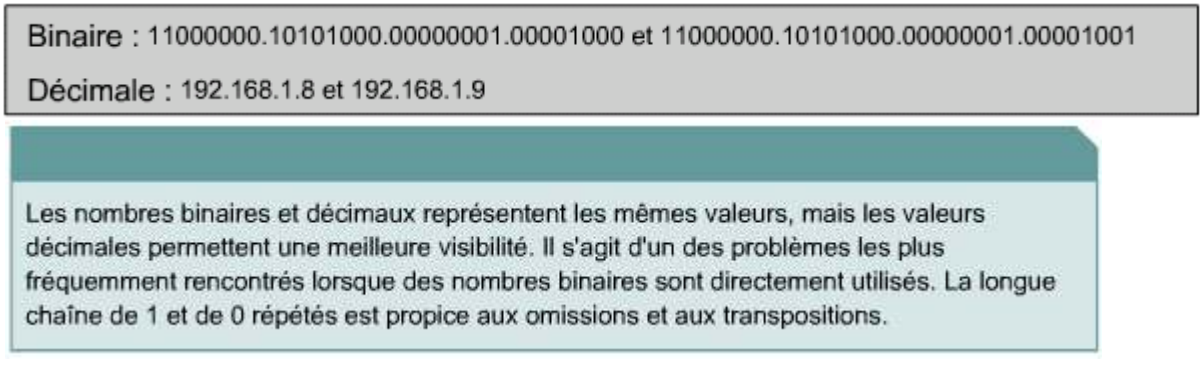
Si tel est le cas, le système doit recevoir plusieurs adresses. Chaque adresse identifie la connexion d'un ordinateur à un réseau différent. Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse associée à un réseau. Cela permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique. La combinaison d'une adresse réseau et d'une adresse hôte crée une adresse unique pour chaque équipement du réseau. Tout ordinateur appartenant à un réseau TCP/IP doit disposer d'un identificateur unique, ou adresse IP. Cette adresse, qui intervient au niveau de la couche 3, permet à un ordinateur de localiser un autre ordinateur sur le réseau. Tous les ordinateurs possèdent également une adresse physique unique, également appelée «adresse MAC». Celle-ci est attribuée par le fabricant de la carte réseau. Les adresses MAC opèrent au niveau de la couche 2 du modèle OSI.

Une adresse IP est une séquence de 32 bits composée de 1 et de 0. La figure 3



donne un exemple de nombre 32 bits. Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous la forme de quatre nombres décimaux séparés par des points. Voici, par exemple, l'adresse IP d'un ordinateur : 192.168.1.2. Un autre ordinateur disposera de l'adresse : 128.10.2.1. Il s'agit de la notation entière avec des points de séparation. Chaque élément d'une adresse s'appelle un octet (toutes les adresses se composent de huit chiffres binaires). Par exemple, l'adresse IP 192.168.1.8 correspond à la valeur 11000000.10101000.00000001.00001000 en notation binaire. La notation entière avec des points de séparation est plus simple à comprendre que la méthode des 1 et des 0 binaires. En outre, elle permet d'éviter un grand nombre d'erreurs de transposition liées à l'utilisation des nombres binaires.

La figure 4


Binaire : 11000000.10101000.00000001.00001000 et 11000000.10101000.00000001.00001001
Décimale : 192.168.1.8 et 192.168.1.9
Les nombres binaires et décimaux représentent les mêmes valeurs, mais les valeurs décimales permettent une meilleure visibilité. Il s'agit d'un des problèmes les plus fréquemment rencontrés lorsque des nombres binaires sont directement utilisés. La longue chaîne de 1 et de 0 répétés est propice aux omissions et aux transpositions.

représente la même valeur sous les formes binaire et décimale. On constate que cette valeur est plus facile à lire exprimée à l'aide de la notation entière avec des points de séparation. Il s'agit d'un des problèmes les plus fréquemment rencontrés avec les nombres binaires. Les longues chaînes de 1 et de 0 répétés sont plus propices aux erreurs.

Au contraire, les adresses exprimées à l'aide de la notation entière avec des points de séparation, telles que 192.168.1.8 et 192.168.1.9, permettent de discerner plus facilement les relations entre les chiffres. Les valeurs binaires 11000000.10101000.00000001.00001000 et 11000000.10101000.00000001.00001001 sont moins facilement identifiables. Il est plus difficile de déterminer que les valeurs binaires sont des nombres séquentiels.

La page suivante traite de la conversion des nombres binaires et décimaux.

9.2 Les adresses Internet

9.2.2 Conversion binaire et décimale

Il existe plusieurs façons de convertir les nombres décimaux en nombres binaires. Cette page décrit l'une de ces méthodes.

Certains étudiants considèreront peut-être que cette méthode n'est pas la plus simple ; tout est question de préférence personnelle.

Lors de la conversion d'un nombre décimal en nombre binaire, vous devez rechercher la puissance de deux la plus proche possible du nombre décimal à convertir, sans dépasser celui-ci. 1

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Dans le cadre d'un processus informatisé, il est plus logique de commencer par les valeurs les plus élevées pouvant être contenues dans un ou deux octets. Comme nous l'avons vu précédemment, le regroupement standard est de huit bits, soit un octet. Cependant, il arrive que la valeur la plus élevée pouvant être contenue dans un octet ne soit pas suffisante par rapport aux valeurs requises. Pour pallier à ce problème, les octets sont regroupés. Au lieu d'avoir deux nombres de huit bits chacun, un seul nombre de 16 bits est créé. Au lieu d'avoir trois nombres de huit bits chacun, un seul nombre de 24 bits est créé. La même règle que celle des nombres de huit bits s'applique. Vous devez ensuite multiplier la valeur de la position précédente par deux pour obtenir la valeur de la colonne actuelle.

Dans la mesure où le traitement informatique est souvent référencé par des octets, il est plus facile de commencer par définir des plages d'octets et d'effectuer le calcul à partir de ces valeurs. 2

Puissance de la position	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}
Valeur décimale	6783	6783	6783	6783	2687	639	639	127	127
Valeur de la position	32768	16384	8192	4096	2048	1024	512	256	128
Compte binaire	0	0	0	1	1	0	1	0	0
Reste	6783	6783	6783	2687	639	639	127	127	127

2^6	2^5	2^4	2^3	2^2	2^1	2^0
127	63	31	15	7	3	1
64	32	16	8	4	2	1
1	1	1	1	1	1	1
63	31	15	7	3	1	0

Entraînez-vous à l'aide, par exemple, de la valeur 6 783. Ce nombre étant supérieur à 255 (valeur maximale pour un seul octet), deux octets sont utilisés. Commencez le calcul à 2^{15}. L'équivalent binaire de la valeur 6 783 est 00011010 01111111.

Le second exemple utilise la valeur 104. Ce nombre étant inférieur à 255, il peut être représenté par un seul octet. L'équivalent binaire de la valeur 104 est 01101000. 3

Puissance de la position	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valeur décimale	104	104	40	8	8	0	0	0
Valeur de la position	128	64	32	16	8	4	2	1
Compte binaire	0	1	1	0	1	0	0	0
Reste	104	40	8	8	0	0	0	0

Cette méthode est valable pour tous les nombres décimaux. Prenons l'exemple du nombre décimal un million. Sachant qu'un million est supérieur à la valeur maximale pouvant être contenue dans deux octets (soit 65 535), au moins trois octets sont nécessaires. En procédant à des multiplications par deux jusqu'à ce que vous atteigniez 24 bits (soit trois octets), vous obtenez la valeur 16 777 215. Autrement dit, la valeur la plus élevée pouvant être contenue dans 24 bits est 16 777 215. Ainsi, en prenant la valeur 24 bits comme point de départ, suivez ce processus jusqu'à atteindre la valeur zéro. En effectuant la procédure décrite, un million (valeur décimale) correspond à 00001111 01000010 01000000 (valeur binaire).

Nombre décimal	Nombre binaire
80	01010000
Essayez un autre nombre.	Vérifiez votre réponse.

La figure 4 **Correct**

comprend des exercices de conversion de nombres décimaux en nombres binaires.

Pour convertir un nombre binaire en nombre décimal, il suffit d'effectuer l'opération en sens inverse. Placez la valeur binaire dans le tableau. Si un 1 est situé dans une position de colonne, ajoutez cette valeur au total. 5

Puissance de la position	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}
Valeur décimale	0	0	0	0	0	0	1024	1024	1024
Valeur de la position	32768	16384	8192	4096	2048	1024	512	256	128
Compte binaire	0	0	0	0	0	1	0	0	0
Reste	0	0	0	0	0	1024	1024	1024	1024

2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
1024	1024	1024	1040	1040	1052	1052
64	32	16	8	4	2	1
0	0	1	1	1	0	1
1024	1024	1040	1048	1052	1052	1053

Convertissez le nombre 00000100 00011101 en représentation décimale. La bonne réponse est: 1 053.

La figure 6

Nombre binaire	Nombre décimal
01001111	79
Essayez un autre nombre.	Vérifiez votre réponse.

Correct

comprend des exercices de conversion de nombres binaires en nombres décimaux.

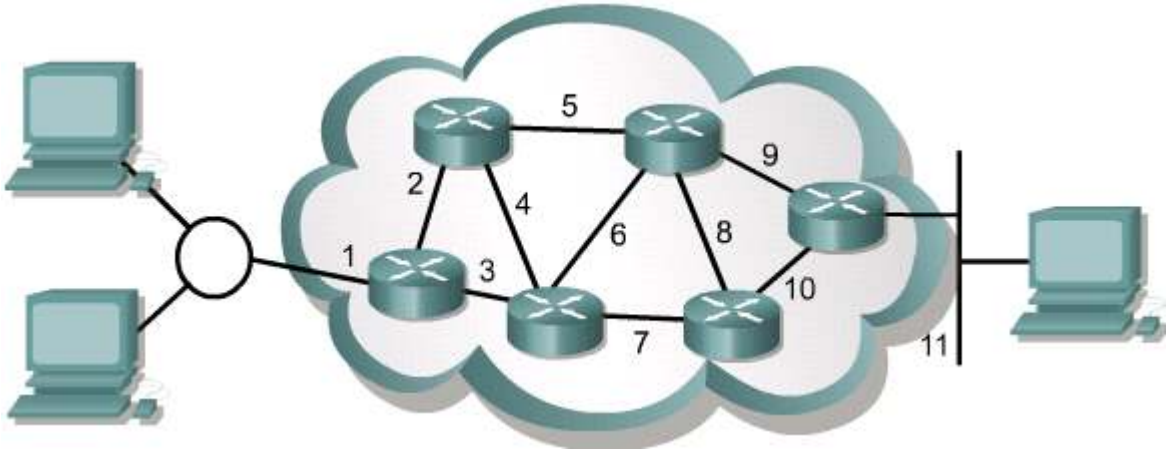
La page suivante traite de l'adressage IPv4.

9.2 Les adresses Internet

9.2.3 Adressage IPv4

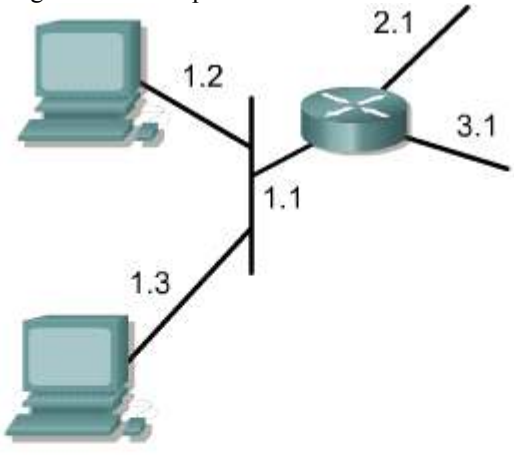
Cette page traite de l'adressage IPv4.

Un routeur fait appel à une adresse IP pour transmettre des paquets du réseau d'origine vers le réseau de destination. Les paquets doivent comporter un identificateur pour les réseaux source et de destination. 1



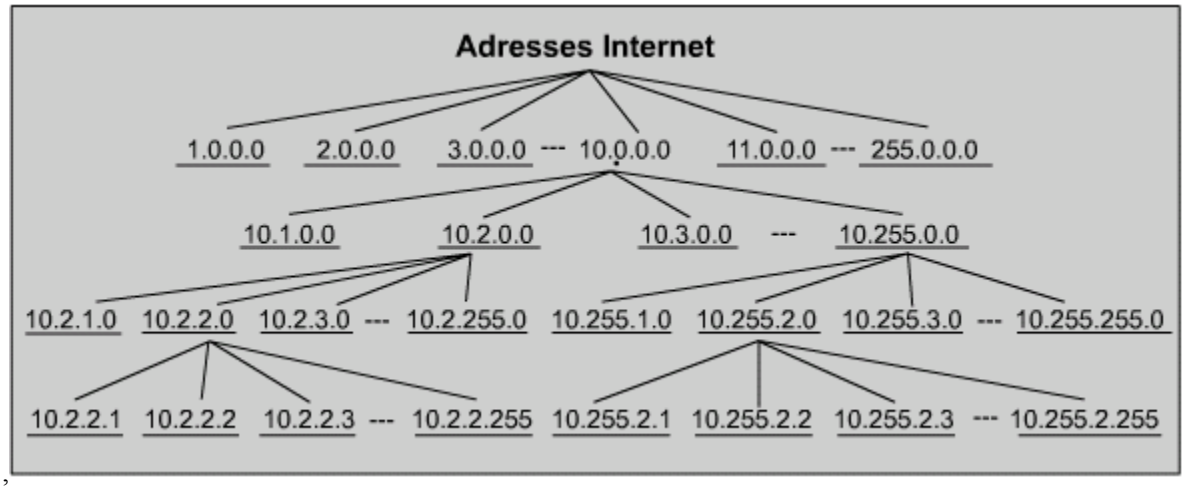
Un routeur utilise l'adresse IP du réseau de destination afin de remettre le paquet au réseau approprié. Lorsque le paquet atteint un routeur connecté au réseau de destination, ce routeur localise l'ordinateur sur le réseau à l'aide de l'adresse IP. Ce système fonctionne pratiquement de la même manière que le système postal national. Une fois le courrier envoyé, le code postal est utilisé pour remettre le courrier au bureau de poste de la ville de destination. Le bureau de poste utilise ensuite la rue pour localiser la destination finale au niveau de la ville.

Chaque adresse IP comporte également deux parties. 2



Réseau	Hôte
1	1 2 3
2	1
3	1

La première partie identifie le réseau auquel le système est connecté et la seconde partie identifie le système. Comme l'illustre la figure 3



,

chaque octet représente une valeur comprise entre 0 et 255. Chacun des octets est subdivisé en 256 groupes, qui se divisent à leur tour en 256 sous-groupes avec 256 adresses chacun. Lorsque vous faites référence à l'adresse d'un groupe directement au-dessus d'un autre groupe de la hiérarchie, tous les groupes qui en dérivent peuvent être référencés en tant qu'une seule et même unité.

On parle dans ce cas de système d'adressage hiérarchique, car il contient plusieurs niveaux. Chaque adresse IP regroupe ces deux identificateurs en un seul nombre. Ce nombre doit être unique, faute de quoi l'acheminement échoue. La première partie identifie l'adresse réseau du système. La seconde, appelée «partie hôte», identifie la machine sur le réseau.

Les adresses IP sont réparties en classes afin de définir des réseaux de grande taille, de taille moyenne et de petite taille. Les adresses IP de classe A sont affectées aux réseaux de grande taille. Les adresses de classe B sont utilisées pour les réseaux de taille moyenne et les adresses IP de classe C pour les réseaux de petite taille. [4] [5]

Classe de l'adresse	Nombre de réseaux	Nombre d'hôtes par réseau
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (multicast)	S.O.	S.O.

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

* La plage d'adresses 127.x.x.x est réservée en tant qu'adresse en mode bouclé, utilisée pour les tests et les diagnostics.

Pour déterminer la partie de l'adresse qui correspond au réseau et celle qui correspond à l'hôte, vous devez d'abord identifier la classe de l'adresse IP.

Les étudiants peuvent utiliser l'activité de média interactive pour mieux appréhender les différentes classes d'adresses.

La page suivante fournit des informations supplémentaires sur les adresses IP de classe A, B, C, D et E.

Activité de média interactive

Glisser-Positionner: Identification des classes d'adresses

À l'issue de cette activité, les étudiants connaîtront les particularités de chaque classe d'adresse Internet.

9.2 Les adresses Internet

9.2.4 Adresses IP de classe A, B, C, D et E

Cette page présente les cinq classes d'adresses IP.

Les adresses IP sont regroupées en classes afin de permettre l'adaptation à des réseaux de différentes tailles et de faciliter leur classification. 1

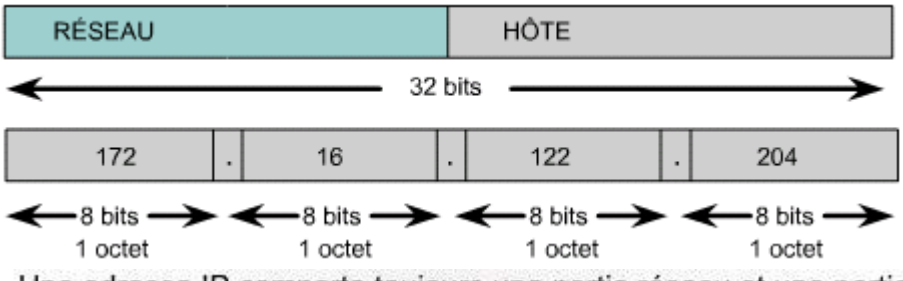
Classe A	Réseau	Hôte		
Octet	1	2	3	4

Classe B :	Réseau		Hôte	
Octet	1	2	3	4

Classe C	Réseau			Hôte
Octet	1	2	3	4

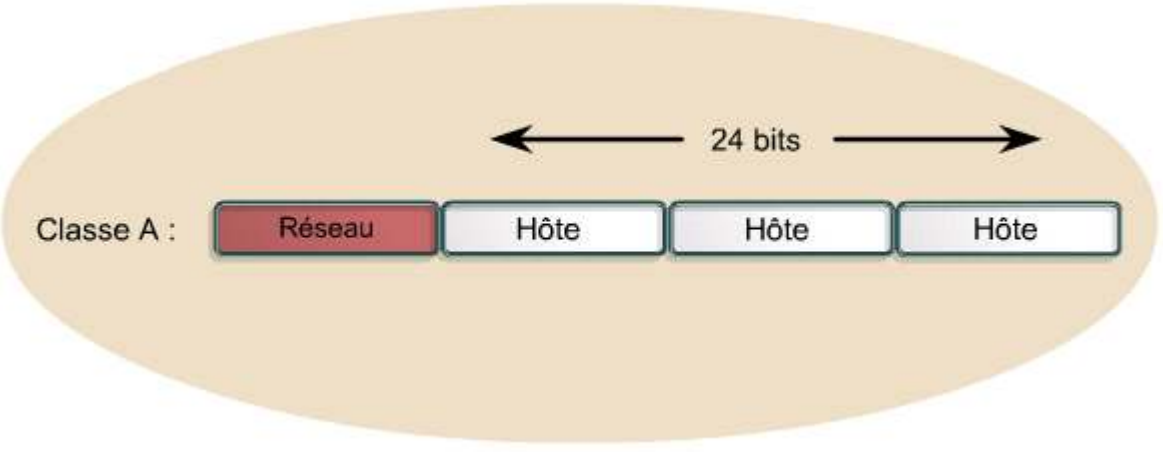
Classe D	Hôte			
Octet	1	2	3	4

Les adresses de classe D sont utilisées pour les groupes de multicast. Il n'est pas nécessaire d'allouer des octets ou des bits pour séparer les adresses réseau et hôte. Les adresses de classe E sont réservées à la recherche.



Une adresse IP comporte toujours une partie réseau et une partie hôte. Dans un modèle d'adressage par classe, cette distinction est effectuée au niveau des frontières entre les octets.

Cette opération est connue sous le nom d'adressage par classes. Chaque adresse IP complète de 32 bits est fractionnée en une partie réseau et une partie hôte. 2



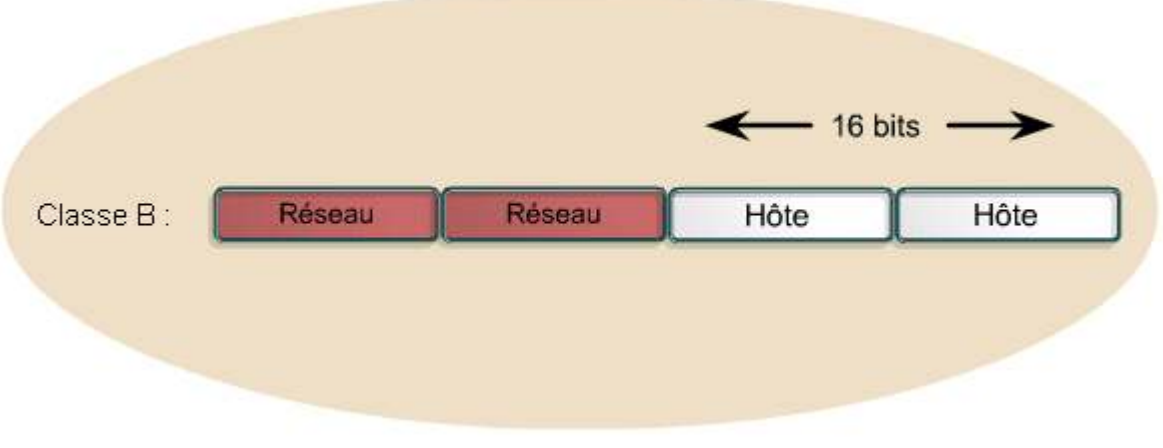
Un bit, ou une séquence de bits, situé en début d'adresse détermine la classe de l'adresse. Il existe cinq classes d'adresses IP, comme l'illustre la figure 8.

L'adresse de classe A est réservée aux réseaux de très grande taille, avec plus de 16 millions d'adresses hôte disponibles. 3Les adresses IP de classe A utilisent uniquement le premier octet pour indiquer l'adresse réseau. Les trois octets suivants sont utilisés pour définir les adresses hôte.

Le premier bit d'une adresse de classe A est toujours 0. Par conséquent, le nombre le plus faible pouvant être représenté est 00000000 (0 en décimal) et le plus élevé est 01111111 (127 en décimal). Les valeurs 0 et 127 sont réservées et ne peuvent pas être utilisées comme adresses réseau. Toute adresse commençant par une valeur comprise entre 1 et 126 dans le premier octet est une adresse de classe A.

Le réseau 127.0.0.0 est réservé pour les tests en bouclage. Les routeurs ou les ordinateurs locaux peuvent utiliser cette adresse pour s'envoyer des paquets. Par conséquent, ce nombre ne peut pas être attribué à un réseau.

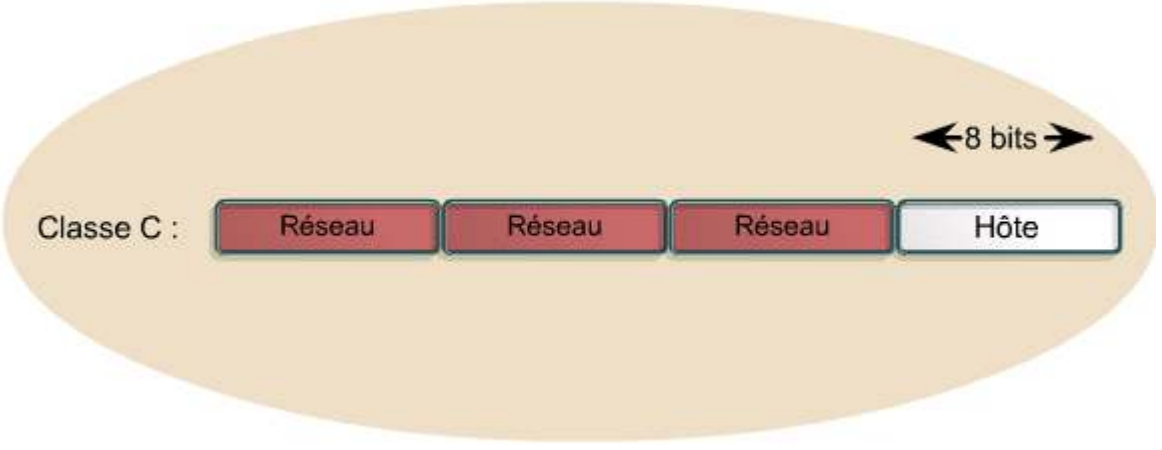
L'adresse de classe B est réservée aux réseaux de taille moyenne ou grande. 4



Les adresses IP de classe B utilisent les deux premiers octets (sur quatre) pour indiquer l'adresse réseau. Les deux octets suivants sont utilisés pour les adresses hôte.

Les deux premiers bits du premier octet d'une adresse de classe B sont toujours 10. Les six bits suivants peuvent être des 1 ou des 0. Par conséquent, dans une classe B, le nombre le plus faible pouvant être représenté est 10000000 (128 en décimal) et le plus élevé est 10111111 (191 en décimal). Toute adresse commençant par une valeur comprise entre 128 et 191 dans le premier octet est une adresse de classe B.

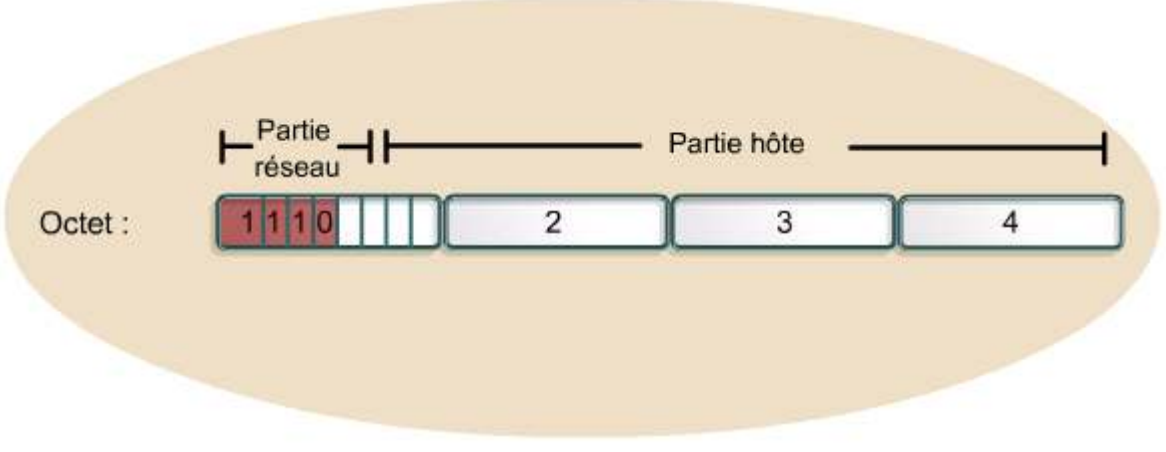
La classe C constitue l'espace le plus utilisé des classes d'adresses initiales. 5



Cet espace d'adressage est réservé aux réseaux de petite taille (254 hôtes maximum).

Une adresse de classe C commence par la valeur binaire 110. Par conséquent, le nombre le plus faible pouvant être représenté est 11000000 (192 en décimal) et le plus élevé est 11011111 (223 en décimal). Toute adresse contenant un nombre compris entre 192 et 223 dans le premier octet est une adresse de classe C.

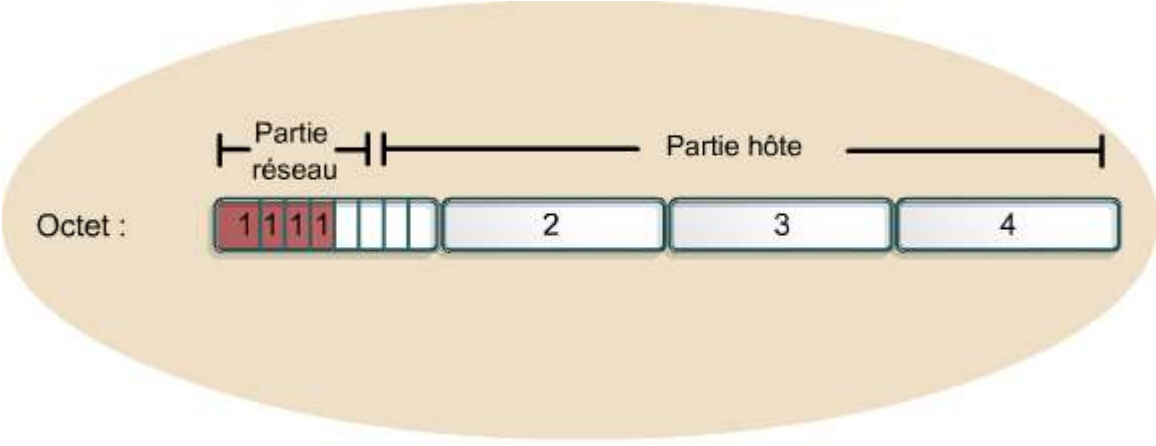
L'adresse de classe D est réservée à la diffusion multicast d'une adresse IP. 6



Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP. Ainsi, une station peut transmettre simultanément un même flux de données vers plusieurs destinataires.

L'espace d'adressage de classe D, tout comme les autres espaces, est lié à des contraintes mathématiques. Les quatre premiers bits d'une adresse de classe D doivent correspondre à 1110. Par conséquent, le premier octet d'une adresse de classe D est compris entre 1100000 et 11101111 (soit 224 et 239 en décimal). Toute adresse IP commençant par une valeur comprise entre 224 et 239 dans le premier octet est une adresse de classe D.

Une adresse de classe E a été définie. 7



Toutefois, le groupe IETF (*Internet Engineering Task Force*) utilise ces adresses à des fins expérimentales. Aucune adresse de classe E n'est disponible sur Internet. Les quatre premiers bits d'une adresse de classe E sont toujours des 1. Par conséquent, le premier octet d'une adresse de classe E est compris entre 11110000 et 11111111 (soit 240 et 255 en décimal).

La figure 8

Classe d'adresses IP	Plage d'adresses IP (premier octet)
Classe A	1-126 (00000001-01111110) *
Classe B :	128-191 (10000000-10111111)
Classe C	192-223 (11000000-11011111)
Classe D	224-239 (11100000-11101111)
Classe E	240-255 (11110000-11111111)

Déterminez la classe d'après le premier octet.
* 127 (011111111) est une adresse de classe A réservée aux tests en mode bouclé et elle ne peut pas être attribuée à un réseau.

indique la plage d'adresses IP du premier octet (sous forme binaire et décimale) de chaque classe d'adresse IP.

La page suivante traite des adresses IP réservées.

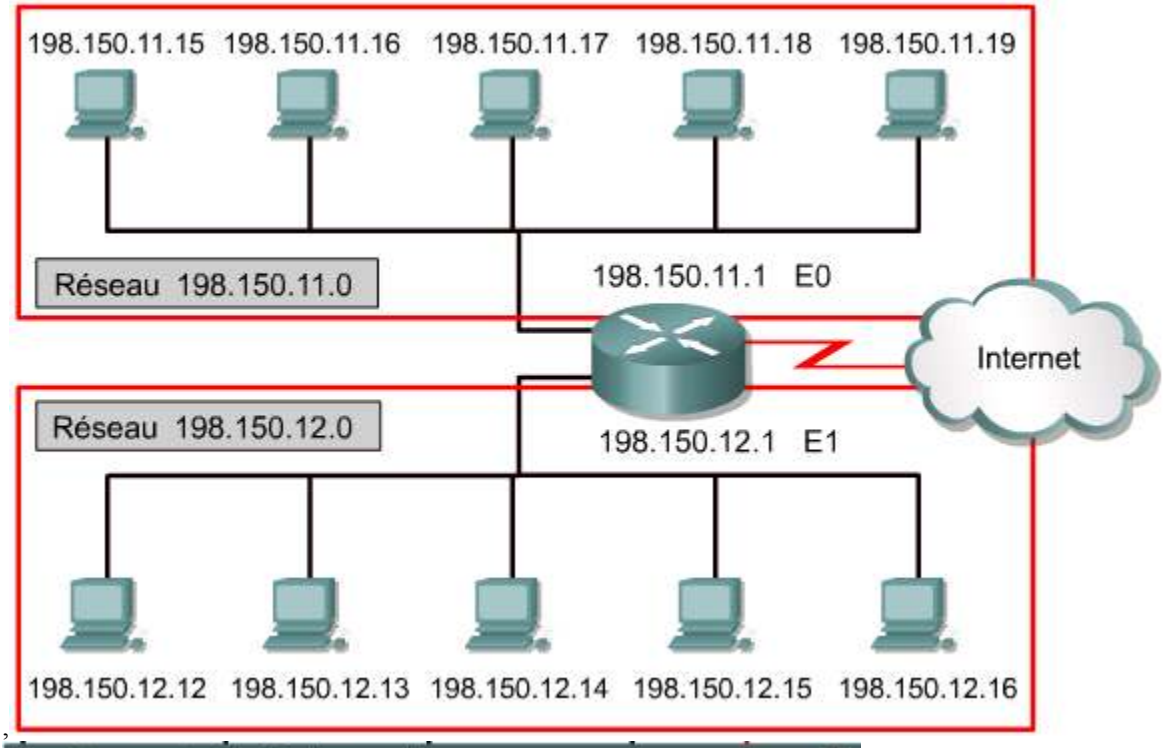
9.2 Les adresses Internet
9.2.5 Adresses IP réservées

Cette page explique les différents types d'adresses IP réservées.

Certaines adresses hôte sont réservées et ne peuvent pas être affectées aux équipements du réseau. Les adresses hôte réservées se composent des éléments suivants:

- **Une adresse réseau** – pour identifier le réseau lui-même.

Dans la figure 1



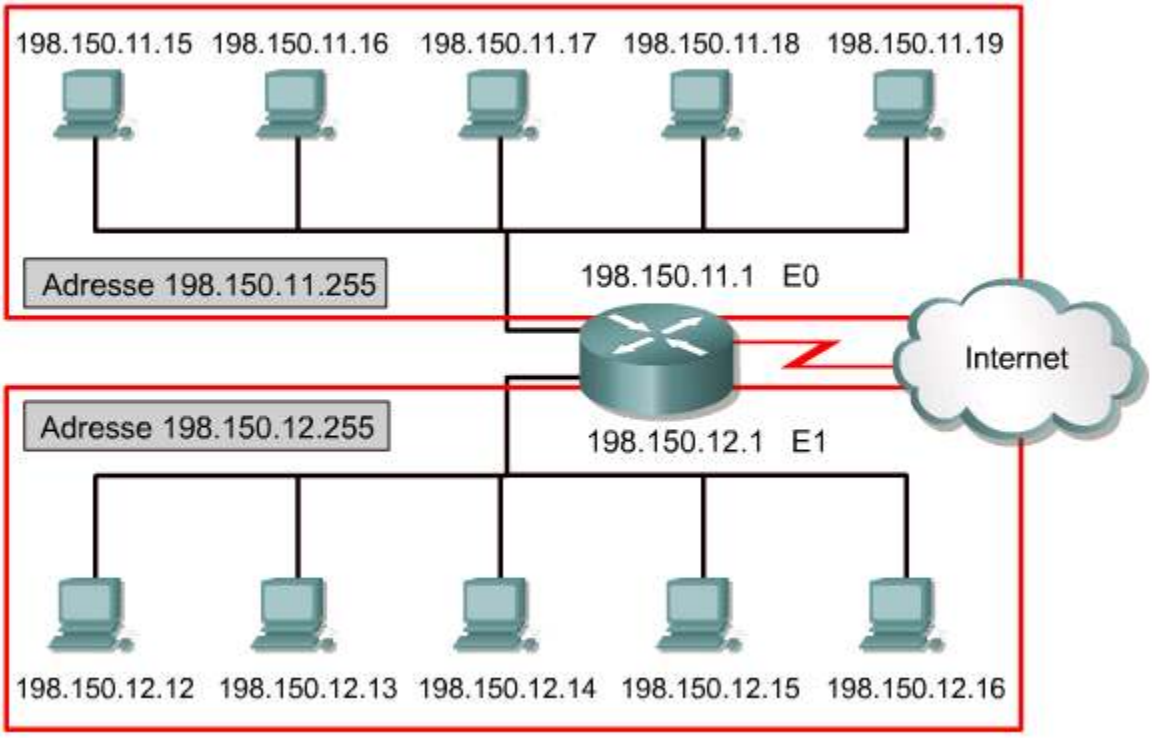
Fenêtre contextuelle (pop up)

La section identifiée par la zone supérieure représente le réseau 198.150.11.0. Les données envoyées à un hôte de ce réseau, de 198.150.11.1 à 198.150.11.254, sont affichées en dehors du réseau local 198.150.11.0. Les numéros d'hôte ne sont pris en compte que lorsque les données se trouvent sur le réseau local. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son numéro de réseau est 198.150.12.0.

la section identifiée par la zone supérieure représente le réseau 198.150.11.0. Les données envoyées à un hôte de ce réseau, de 198.150.11.1 à 198.150.11.254, seront visibles en dehors du réseau local sous la forme 198.159.11.0. Les numéros d'hôte ne sont pris en compte que lorsque les données se trouvent sur le réseau local. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son numéro de réseau est 198.150.12.0.

- **Une adresse de broadcast** – pour diffuser des paquets vers tous les équipements d'un réseau.

Dans la figure 2

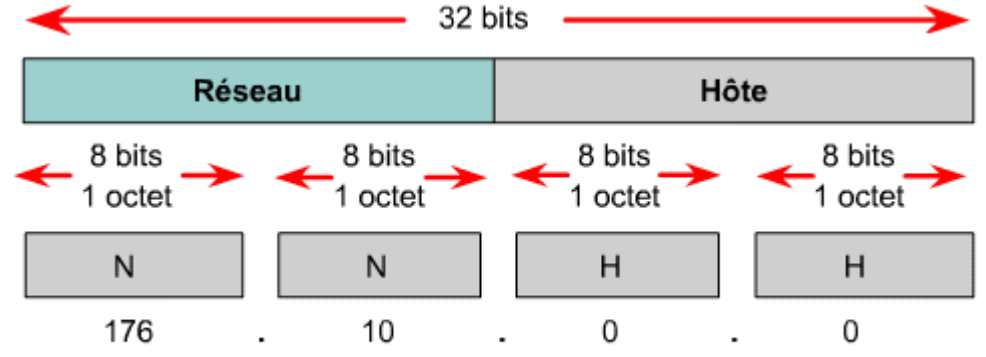


Fenêtre contextuelle (pop up)

La section identifiée par la zone supérieure représente l'adresse de broadcast 198.150.11.255. Les données envoyées à l'adresse de broadcast seront lues par un hôte du réseau, de 198.150.11.1 à 198.150.11.254. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son adresse de broadcast est 198.150.12.255.

la section identifiée par la zone supérieure représente l'adresse de broadcast 198.150.11.255. Les données envoyées à l'adresse de broadcast seront lues par tous les hôtes du réseau, de 198.150.11.1 à 198.150.11.254. Le LAN inclus dans la zone inférieure est traité de la même façon que le LAN supérieur, mais son adresse de broadcast est 198.150.12.255.

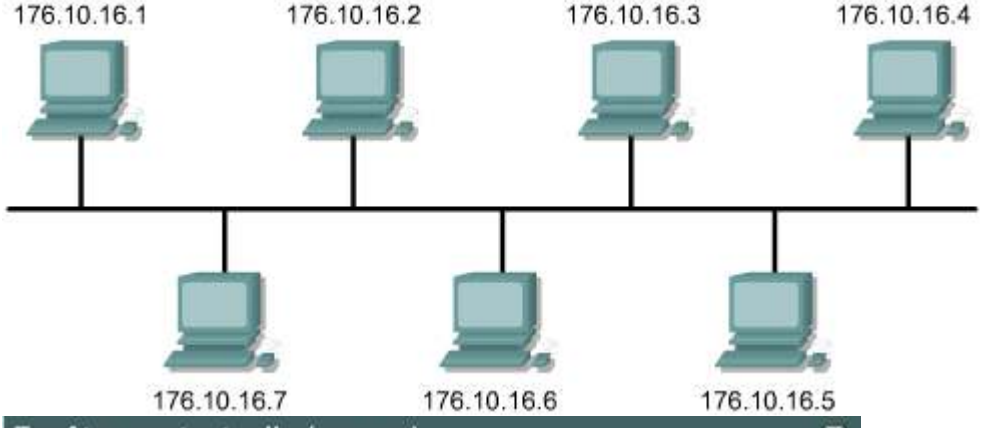
Une adresse IP dont tous les bits hôte sont occupés par des 0 binaires est réservée pour l'adresse réseau. Dans un réseau de classe A, 113.0.0.0 est l'adresse IP du réseau (également connue sous le nom d'ID réseau) comprenant l'hôte 113.1.2.3. Un routeur utilise l'adresse IP du réseau pour acheminer des données sur Internet. Dans un réseau de classe B, l'adresse 176.10.0.0 est une adresse réseau, comme l'illustre la figure 3



Adresse réseau (bits d'hôte = uniquement des 0)

Cette adresse de classe B ne comporte que des bits définis sur 0. C'est pourquoi elle est identifiée en tant qu'adresse réseau.

Dans une adresse réseau de classe B, les deux premiers octets constituent la partie réseau. Les deux derniers octets contiennent des 0, parce que ces 16 bits sont des numéros d'hôtes et sont utilisés pour identifier les équipements reliés au réseau. L'adresse IP, 176.10.0.0, est un exemple d'adresse réseau. Cette adresse n'est jamais affectée comme adresse hôte. L'adresse hôte d'un équipement sur le réseau 176.10.0.0 peut être 176.10.16.1. Dans cet exemple, «176.10» représente la partie réseau, tandis que « 16.1 » représente la partie hôte. 4



Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 va utiliser une transmission Unicast pour communiquer avec l'ordinateur 176.10.16.3.

L'ordinateur 176.10.16.1 prépare les données à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.

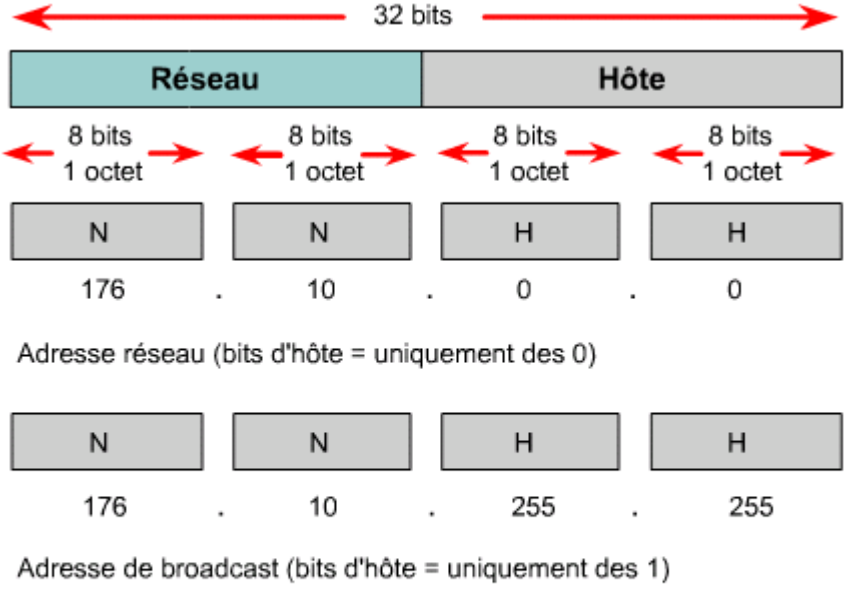
L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Les trames ne sont plus prises en compte par les ordinateurs, à l'exception de l'ordinateur 176.10.16.3, car elles ne correspondent pas à

l'adresse MAC de destination des trames entrantes. C'est pourquoi cette transmission est appelée transmission Unicast. Seul l'ordinateur dont l'adresse correspond continue à traiter la trame, et chaque adresse IP étant unique, un seul ordinateur va accepter les données.
L'ordinateur 176.10.16.3 traite les données provenant des trames de données de l'ordinateur 176.10.16.1 et prépare une réponse pour l'ordinateur 176.10.16.1. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.
L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.
À nouveau, tous les hôtes du même segment analysent les trames entrantes.
Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.

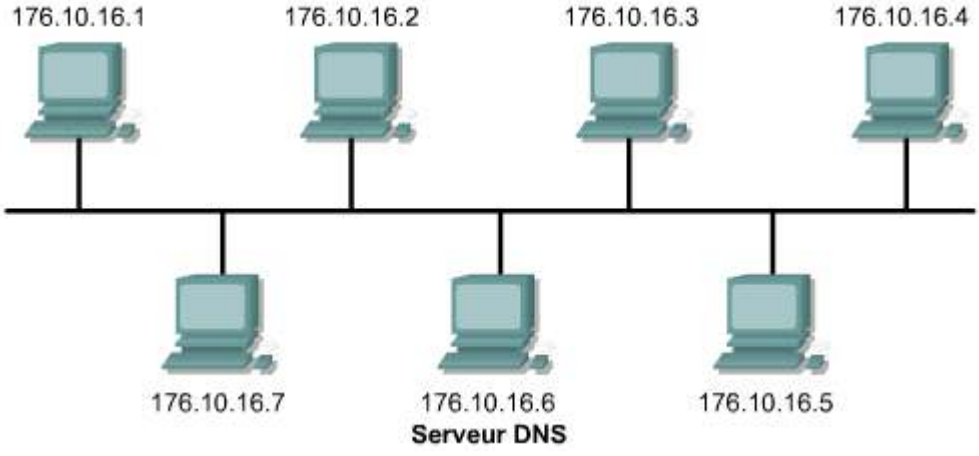
Une adresse de broadcast est requise afin de pouvoir envoyer les données à tous les équipements d'un réseau. 5

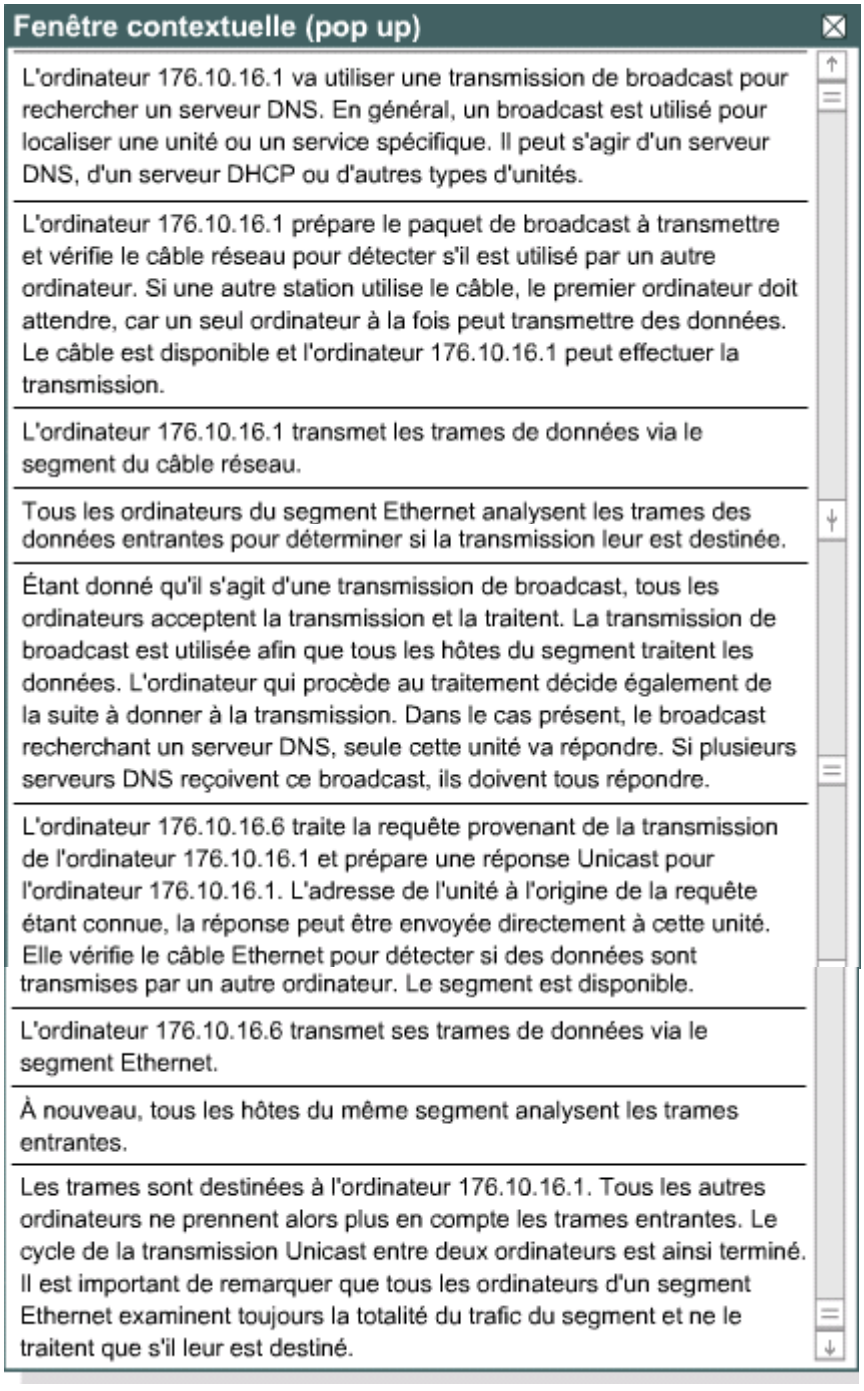


Cette adresse de classe B est l'adresse de broadcast de ce réseau. Lorsque des paquets sont reçus avec cette adresse de destination, les données sont traitées par chaque ordinateur.

On parle de broadcast lorsqu'une source envoie des données à tous les équipements d'un réseau. Pour vérifier que tous les équipements d'un réseau traitent un tel message de broadcast, la source doit utiliser une adresse IP que tous les équipements peuvent reconnaître et traiter. Les adresses IP de broadcast se terminent par des 1 binaires dans toute la partie hôte de l'adresse.

Dans l'exemple 176.10.0.0, les 16 derniers bits forment le champ hôte (ou partie hôte) de l'adresse.



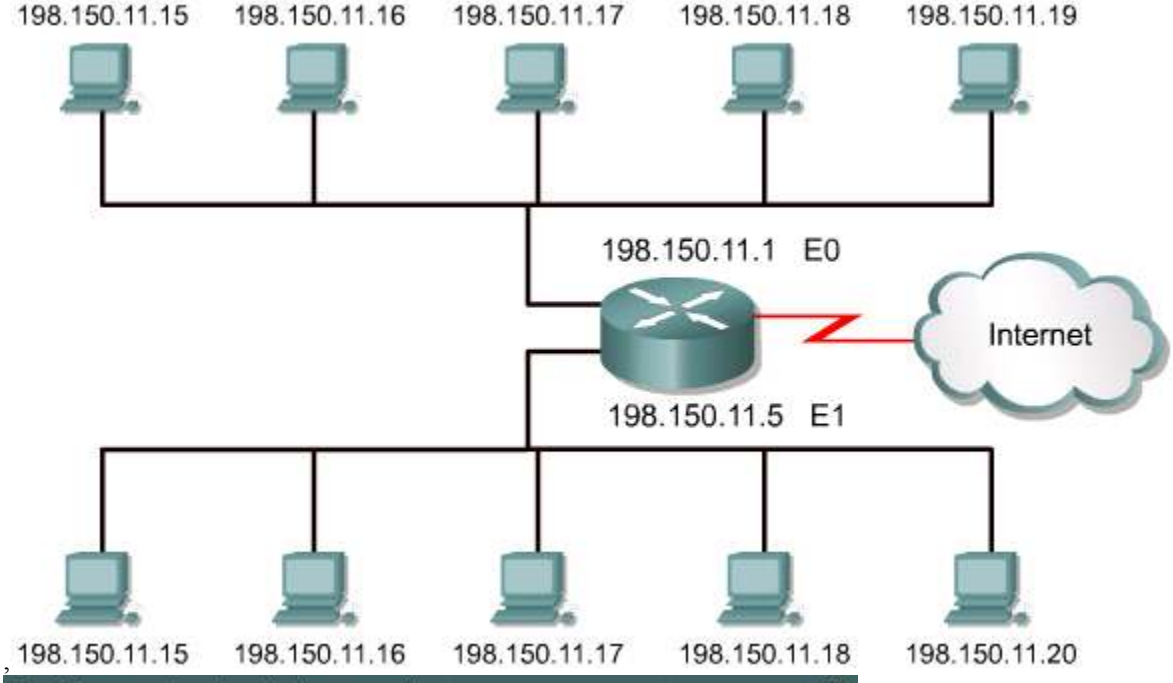

Fenêtre contextuelle (pop up)
L'ordinateur 176.10.16.1 va utiliser une transmission de broadcast pour rechercher un serveur DNS. En général, un broadcast est utilisé pour localiser une unité ou un service spécifique. Il peut s'agir d'un serveur DNS, d'un serveur DHCP ou d'autres types d'unités.
L'ordinateur 176.10.16.1 prépare le paquet de broadcast à transmettre et vérifie le câble réseau pour détecter s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, le premier ordinateur doit attendre, car un seul ordinateur à la fois peut transmettre des données. Le câble est disponible et l'ordinateur 176.10.16.1 peut effectuer la transmission.
L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.
Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.
Étant donné qu'il s'agit d'une transmission de broadcast, tous les ordinateurs acceptent la transmission et la traitent. La transmission de broadcast est utilisée afin que tous les hôtes du segment traitent les données. L'ordinateur qui procède au traitement décide également de la suite à donner à la transmission. Dans le cas présent, le broadcast recherchant un serveur DNS, seule cette unité va répondre. Si plusieurs serveurs DNS reçoivent ce broadcast, ils doivent tous répondre.
L'ordinateur 176.10.16.6 traite la requête provenant de la transmission de l'ordinateur 176.10.16.1 et prépare une réponse Unicast pour l'ordinateur 176.10.16.1. L'adresse de l'unité à l'origine de la requête étant connue, la réponse peut être envoyée directement à cette unité. Elle vérifie le câble Ethernet pour détecter si des données sont transmises par un autre ordinateur. Le segment est disponible.
L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.
À nouveau, tous les hôtes du même segment analysent les trames entrantes.
Les trames sont destinées à l'ordinateur 176.10.16.1. Tous les autres ordinateurs ne prennent alors plus en compte les trames entrantes. Le cycle de la transmission Unicast entre deux ordinateurs est ainsi terminé. Il est important de remarquer que tous les ordinateurs d'un segment Ethernet examinent toujours la totalité du trafic du segment et ne le traitent que s'il leur est destiné.

Le broadcast envoyé à tous les équipements du réseau comporterait l'adresse de destination 176.10.255.255, sachant que 255 correspond à la valeur décimale d'un octet contenant 11111111.

La page suivante traite des adresses IP publiques et privées.

Cette page présente les adresses IP publiques et privées.

La stabilité d'Internet découle directement de l'unicité des adresses réseau publiques. Dans la figure 1



Fenêtre contextuelle (pop up)

Le modèle d'adressage réseau est incorrect. L'adresse réseau des deux réseaux est 198.150.11.0. Dans cet exemple, lorsque les transmissions de données atteignent le routeur, comment ce dernier doit-il les orienter ? Si cette action était autorisée, le trafic du réseau serait considérablement plus important et irait à l'encontre de la fonction de base du routeur. L'adresse de chaque unité d'un réseau doit être unique.

le modèle d'adressage réseau est incorrect. En effet, l'adresse 198.150.11.0 est la même pour les deux réseaux. Dès lors, le routeur n'est pas capable de transférer correctement les paquets de données. L'utilisation d'adresses IP réseau identiques double empêche le routeur de sélectionner le meilleur chemin. L'adresse de chaque équipement d'un réseau doit être unique.

Il fallait donc trouver un moyen de veiller à cela. À l'origine, un organisme portant le nom d'InterNIC (*Internet Network Information Center*) était chargé de cette vérification. Celui-ci n'existe plus et a été remplacé par l'IANA (*Internet Assigned Numbers Authority*). L'IANA gère scrupuleusement les adresses IP disponibles afin de garantir qu'une même adresse publique n'est pas utilisée deux fois. En cas de doublons d'adresses, Internet devient instable et ses capacités à transmettre des datagrammes sur le réseau sont compromises.

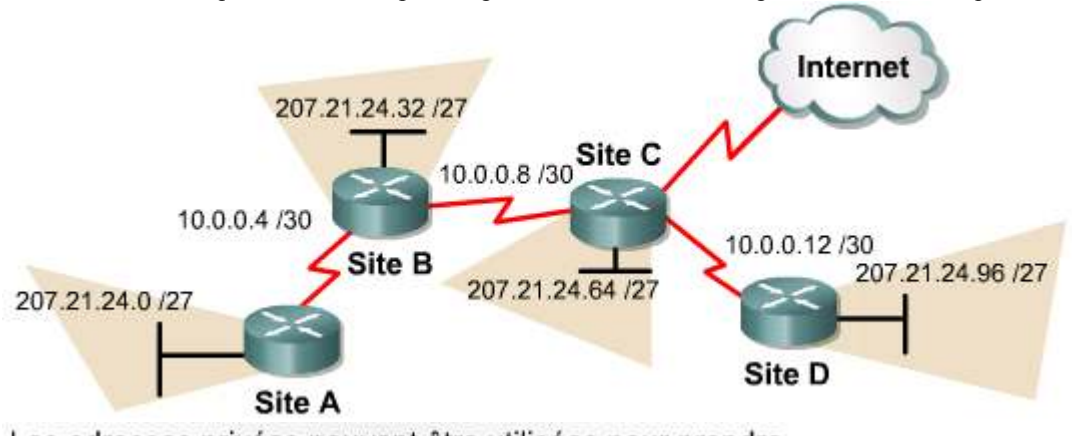
Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique. Les adresses IP publiques sont mondiales et normalisées. Tous les ordinateurs connectés à Internet se conforment au système. Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation.

Avec la croissance rapide d'Internet est apparu le problème de pénurie d'adresses IP publiques. Pour résoudre ce problème, de nouveaux systèmes d'adressage, notamment le routage CIDR (*Classless interdomain routing*) et la norme IPv6, ont été développés. Ces systèmes seront traités ultérieurement dans le cours.

Les adresses IP privées constituent une solution de rechange au problème de pénurie des adresses IP publiques. Comme précédemment indiqué, les hôtes d'un réseau public doivent disposer d'une adresse IP unique. Néanmoins, les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse hôte, dès lors que chacun des hôtes du réseau privé est unique. Un grand nombre de réseaux privés coexistent avec les réseaux publics. Cependant, il est vivement déconseillé d'avoir recours à un réseau privé utilisant une adresse quelconque, car ce réseau peut être connecté à Internet. La spécification RFC 1918 réserve trois blocs d'adresses IP pour une utilisation privée et interne. 2

Classe	Plage d'adresses internes RFC 1918
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Ceux-ci se composent d'une classe A, d'une plage d'adresses de classe B et d'une plage d'adresses de classe C. Les adresses contenues dans ces plages ne sont pas acheminées sur les routeurs du backbone d'Internet. Ces routeurs Internet les rejettent immédiatement. Dans le cadre de l'adressage d'un intranet non public, d'un TP ou d'un réseau domestique, ces adresses privées peuvent être utilisées à la place d'adresses uniques mondiales. 3



Les adresses privées peuvent être utilisées pour prendre en charge les liaisons série point-à-point sans gaspiller les adresses IP réelles.

Les adresses IP privées peuvent être mélangées aux adresses publiques, comme indiqué dans le graphique. Ainsi, le nombre d'adresses utilisées pour les connexions internes sera le même.

La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé «NAT» (*Network Address Translation*). L'équipement chargé d'exécuter le système NAT est généralement un routeur. Le système NAT, ainsi que le routage CIDR et la norme IPv6 seront abordés plus tard dans le cursus.

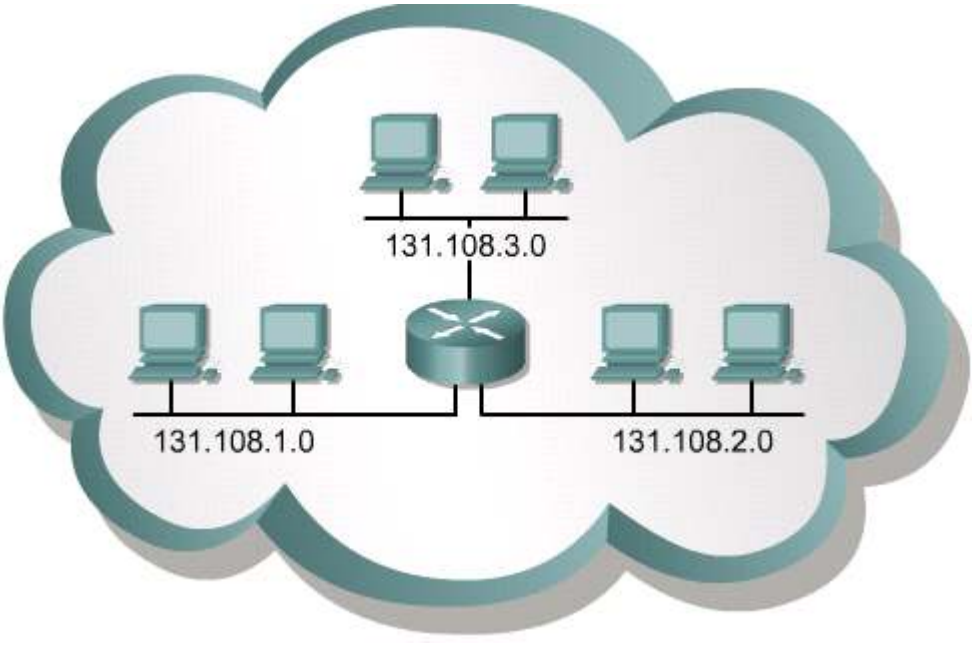
La page suivante contient des informations sur les sous-réseaux.

9.2 Les adresses Internet

9.2.7 Introduction aux sous-réseaux

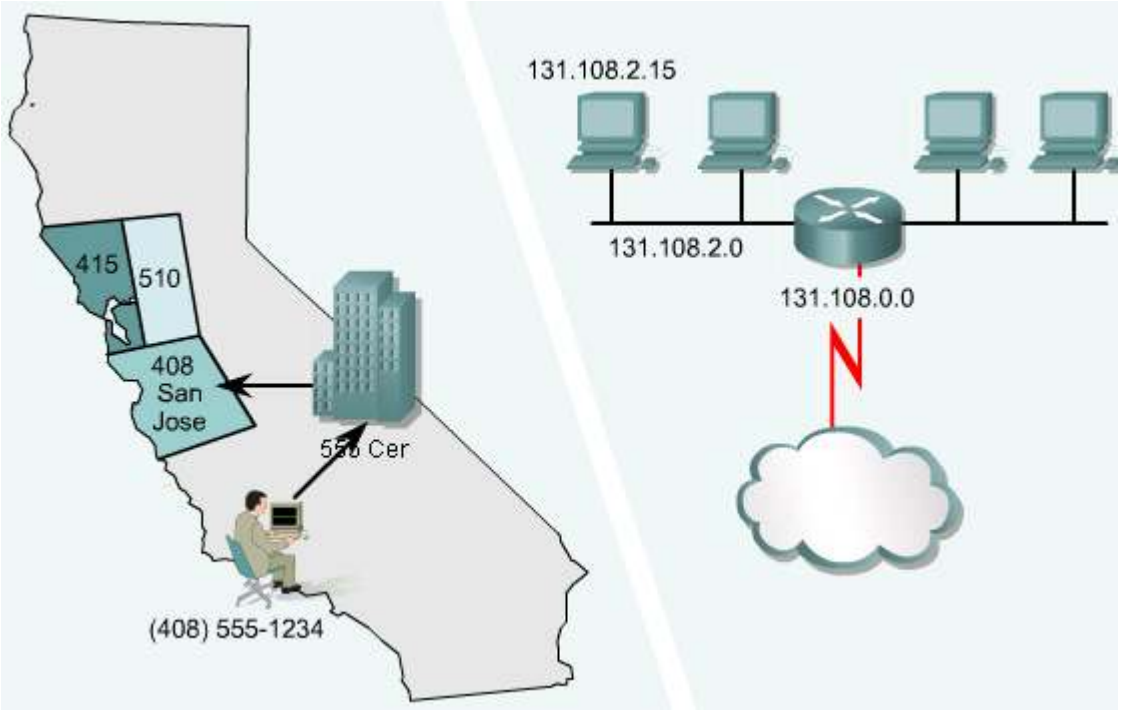
Cette page explique la procédure de découpage en sous-réseaux afin de gérer les adresses IP.

La décomposition en sous-réseaux (subnetting) est une méthode utilisée pour gérer les adresses IP. Comme le montre la figure 1



,

le réseau 131.108.0.0 est décomposé en trois sous-réseaux, le 131.108.1.0, le 131.108.2.0 et le 131.108.3.0. Cette méthode, basée sur la fragmentation de classes d'adresses réseau entières en composants plus petits, a permis d'éviter la pénurie d'adresses IP. Il est impossible de traiter du protocole TCP/IP sans aborder la question des sous-réseaux. En tant qu'administrateur système, il est primordial d'appréhender la notion de découpage en sous-réseaux afin de pouvoir subdiviser un LAN et y identifier les différents réseaux. Dans le cas de réseaux de petite taille, il n'est pas toujours utile de créer des sous-réseaux. En revanche, dans le cadre des réseaux de grande à très grande taille, cette opération s'impose. 2



Le découpage d'un réseau en sous-réseaux implique l'utilisation du masque de sous-réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces. On pourrait établir une comparaison avec le système téléphonique américain qui se compose d'un indicatif régional, d'un indicatif de central et de numéros locaux.

L'administrateur système doit réfléchir aux problèmes suivants lors de l'évolution d'un réseau: il est essentiel de définir le nombre de sous-réseaux ou de réseaux requis, ainsi que le nombre d'hôtes requis par réseau. En utilisant des sous-réseaux, le réseau n'est pas limité aux masques de réseau de classe A, B ou C par défaut. En outre, la conception du réseau est plus flexible.

Les adresses de sous-réseau contiennent une partie réseau, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine pour l'ensemble du réseau. L'administrateur réseau jouit d'une grande souplesse d'adressage dans la mesure où il peut déterminer la façon dont la partie hôte d'origine sera subdivisée pour créer les nouveaux champs de sous-réseau et d'hôte.

Pour créer une adresse de sous-réseau, l'administrateur réseau emprunte des bits au champ d'hôte et les désigne comme champ de sous-réseau. 3

Nombre de bits emprunté au champ hôte pour créer des sous-réseaux	Nombre de sous-réseaux	Nombre d'hôtes de classe A par sous-réseau	Nombre d'hôtes de classe B par sous-réseau	Nombre d'hôtes de classe C par sous-réseau
2	2	4,194,302	16,382	62
3	6	2,097,150	8,190	30
4	14	1,048,574	4,094	14
5	30	524,286	2,046	6
6	62	262,142	1,022	2
7	126	131,070	510	-
8	254	65,534	254	-

Le nombre minimal de bits pouvant être empruntés est deux. Lors de la création d'un sous-réseau pour lequel un seul bit a été emprunté, le numéro de réseau est .0, tandis que le numéro de broadcast est le réseau .255. Le nombre maximal de bits pouvant être empruntés est égal à tout nombre laissant au moins deux bits disponibles pour le numéro d'hôte.

Les étudiants peuvent effectuer l'activité de TP pour se familiariser avec les différentes classes d'adresses IP.

La page suivante traite de la norme IP Version 6 (IPv6).

Activité de TP

Exercice: Notions de base sur l'adressage IP

L'objectif de ce TP est de nommer les cinq classes d'adresses IP et de décrire les caractéristiques et l'utilisation de ces différentes classes.

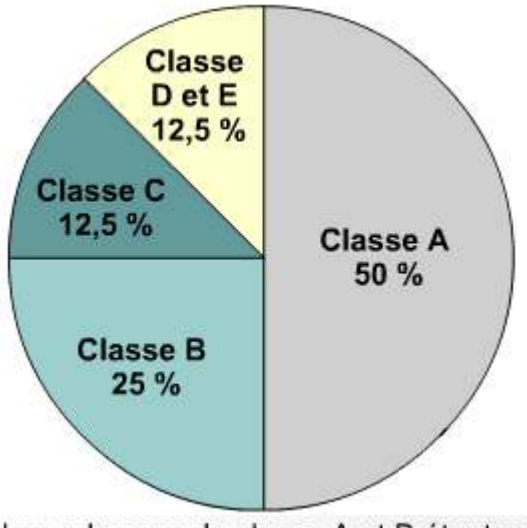
9.2 Les adresses Internet

9.2.8 Comparaison entre IPv4 et IPv6

L'objectif de cette page est de comparer les normes IPv4 et IPv6.

Lors de son adoption dans les années 80, le protocole TCP/IP s'appuyait sur un système d'adressage à deux niveaux. Ses possibilités d'évolution étaient alors parfaitement adaptées. Malheureusement, ses concepteurs ne pouvaient pas prévoir qu'il allait soutenir un réseau mondial dédié à l'information, aux échanges commerciaux et au divertissement. Dans les années 80, la stratégie d'adressage proposée par la version IPv4 s'avérait relativement évolutive. Néanmoins, elle ne réussit pas à satisfaire les exigences liées à l'attribution des adresses.

Les adresses de classe A et B représentent 75% de l'espace d'adresses IPv4. Toutefois, moins de 17 000 organisations peuvent recevoir un numéro de réseau de classe A ou B. 1



Les adresses de classe A et B étant pratiquement toutes utilisées, les adresses de classe C (12,5 % de l'espace total) peuvent être attribuées aux nouveaux réseaux.

Le nombre d'adresses réseau de classe C est nettement plus important que celui des adresses de classe A et B, bien qu'il ne représente que 12,5 % des quatre milliards d'adresses IP disponibles.

Malheureusement, seuls 254 hôtes utilisables sont disponibles sur un réseau de classe C. Ce nombre ne permet pas de satisfaire les besoins des organisations plus importantes qui ne peuvent pas obtenir d'adresses de classe A ou B. S'il existait davantage d'adresses de classe A, B et C, un nombre trop élevé d'adresses réseau risquerait de provoquer l'arrêt des routeurs, du fait du volume trop important des tables de routage requises pour stocker les routes permettant d'atteindre les différents réseaux.

Dès 1992, le groupe IETF (*Internet Engineering Task Force*) a identifié deux problèmes :

- La diminution inquiétante des adresses réseau IPv4 disponibles. À l'époque, l'espace d'adresses de classe B était sur le point d'être saturé.
- La hausse importante et rapide du volume des tables de routage d'Internet en raison de l'augmentation du nombre de connexions des réseaux de classe C. Ce déferlement de nouvelles informations réseau constituait une menace pour le bon fonctionnement des routeurs Internet.

Au cours des deux dernières décennies, plusieurs extensions de la norme IPv4 ont été développées. Celles-ci étaient spécifiquement conçues pour optimiser l'espace des adresses 32 bits. Deux des plus significatives, à savoir les masques de sous-réseau et le routage CIDR (*Classless interdomain routing*), feront l'objet d'une étude plus approfondie dans les leçons suivantes.

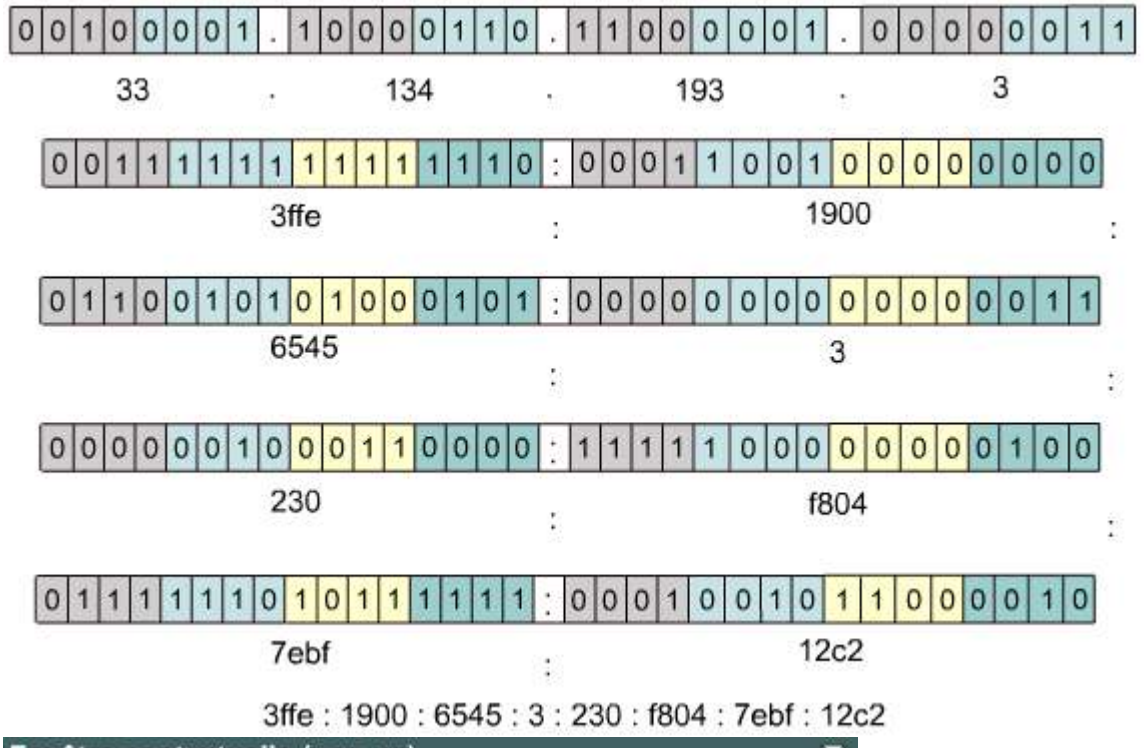
Entre-temps, une version encore plus flexible et évolutive de la norme IP (IPv6) a fait son apparition. 2

Version 4 du protocole IP (IPv4)	4 octets
11010001.11011100.11001001.01110001	
209.156.201.113	
4 294 467 295 adresses IP	

Version 6 du protocole IP (IPv6)	16 octets
10100101.00100100.01110010.11010011	
00101100.10000000.11011101.00000010	
00000000.00101001.11101100.01111010	
00000000.00101011.11101010.01110011	
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73	
3,4 x 10^{38} adresses IP	

IPv6 encode les adresses sur 128 bits au lieu de 32 (en utilisant des nombres hexadécimaux), ce qui porte le nombre d'adresses possibles à 340 x 10^{36}. Cette version devrait ainsi couvrir l'intégralité des besoins en communication pour les années à venir.

La figure 3



Fenêtre contextuelle (pop up)

Les adresses IPv4, qui sont les plus fréquentes, ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Toutefois, les adresses IPv6 ont une longueur de 128 bits et sont exprimées au format hexadécimal avec deux-points de séparation. Les deux-points séparent les champs de 16 bits. Les zéros de tête peuvent être omis dans chaque champ, comme dans l'exemple ci-dessus, où " 0003 " est écrit " 3 ".

présente les adresses IPv4 et IPv6. Les adresses IPv4 ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Les adresses IPv6 ont une longueur de 128 bits et constituent un identifiant pour une interface ou un ensemble d'interfaces. Les adresses IPv6 sont affectées à des interfaces et non à des nœuds. Dans la mesure où chaque interface appartient à un nœud unique, toutes les adresses d'unicast attribuées aux interfaces du nœud peuvent être utilisées comme identifiant du nœud. Les adresses IPv6 sont exprimées au format hexadécimal avec des deux-points de séparation. Les champs IPv6 ont une longueur de 16 bits. Afin de faciliter la lecture des adresses, il est possible d'omettre les zéros de tête dans chaque champ. Le champ «0003» est écrit «3». La représentation abrégée IPv6 de 128 bits consiste en huit nombres de 16 bits, représentés par quatre chiffres hexadécimaux.

Après des années de planification et de développement, IPv6 s'implante doucement sur les réseaux et devrait progressivement supplanter le protocole IPv4.

Cette page termine la leçon. La leçon suivante décrit la procédure d'obtention d'une adresse IP. La première page traite des adresses Internet.

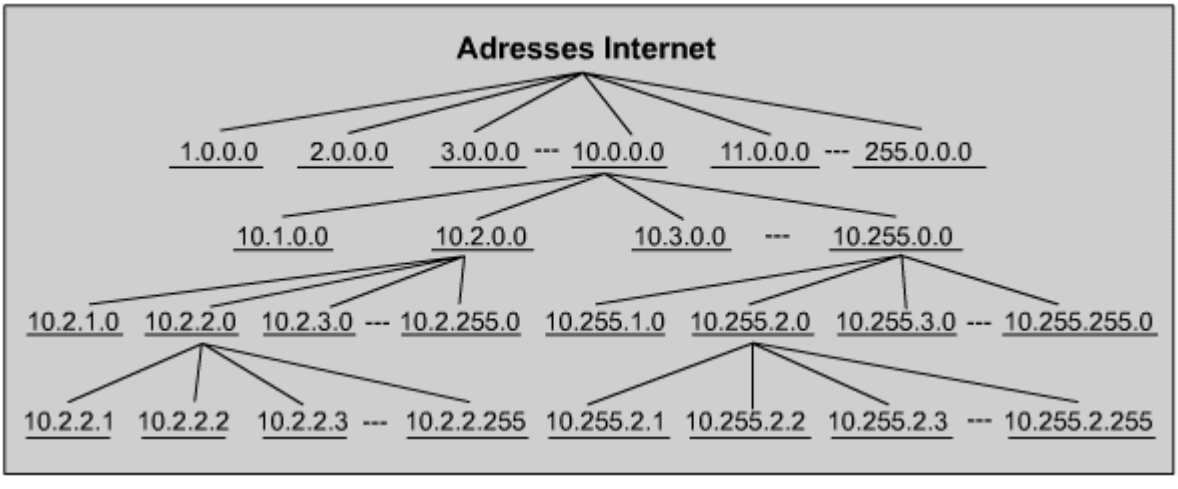
9.3 Obtention d'une adresse IP

9.3.1 Obtention d'une adresse Internet

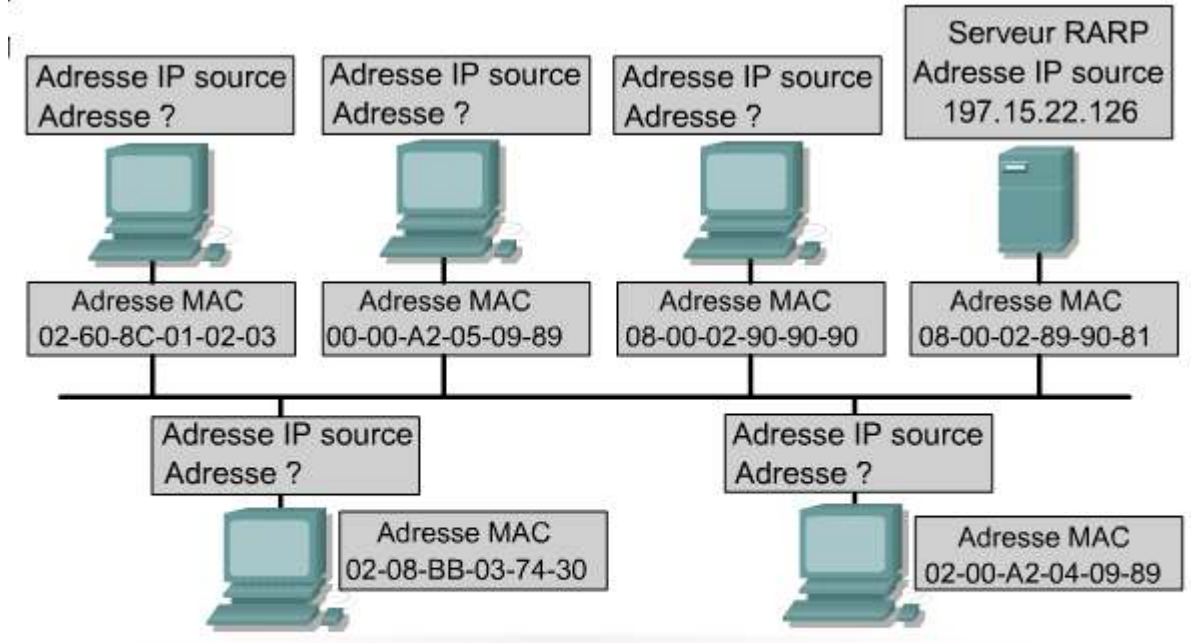
Cette page explique comment obtenir une adresse Internet.

Un hôte réseau doit se procurer une adresse unique mondialement afin de se connecter à Internet. L'adresse physique ou MAC d'un hôte n'est significative que localement, car elle identifie l'hôte sur le réseau local. Cette adresse opérant au niveau de la couche 2, le routeur ne l'utilise pas pour transmettre des données au-delà du réseau local.

Les adresses IP sont les adresses les plus fréquemment utilisées pour les communications Internet. Ce protocole, basé sur un système d'adressage hiérarchique, permet d'associer des adresses individuelles entre elles et de les traiter en tant que groupes. Ce groupement d'adresses assure un transfert efficace des données sur Internet. 1



Les administrateurs réseau font appel à deux méthodes différentes pour affecter les adresses IP. Il s'agit des méthodes statique et dynamique. L'adressage statique ainsi que trois variantes d'adressage dynamique seront abordés ultérieurement dans cette leçon. Quelle que soit la méthode choisie, deux interfaces ne peuvent jamais avoir la même adresse IP. Lorsque deux hôtes utilisent la même adresse IP, ils risquent de ne pas fonctionner correctement en raison d'un conflit d'adresses. Comme l'illustre la figure 2



Les hôtes bénéficient d'une adresse physique car ils comportent une carte réseau qui permet d'accéder au média physique. Les adresses IP doivent être attribuées à l'hôte selon l'une des méthodes possibles. L'attribution des adresses IP peut être statique ou dynamique.

les hôtes sont dotés d'une adresse physique par le biais de la carte réseau qui permet d'accéder au média physique.

La page suivante porte sur l'attribution statique des adresses IP.

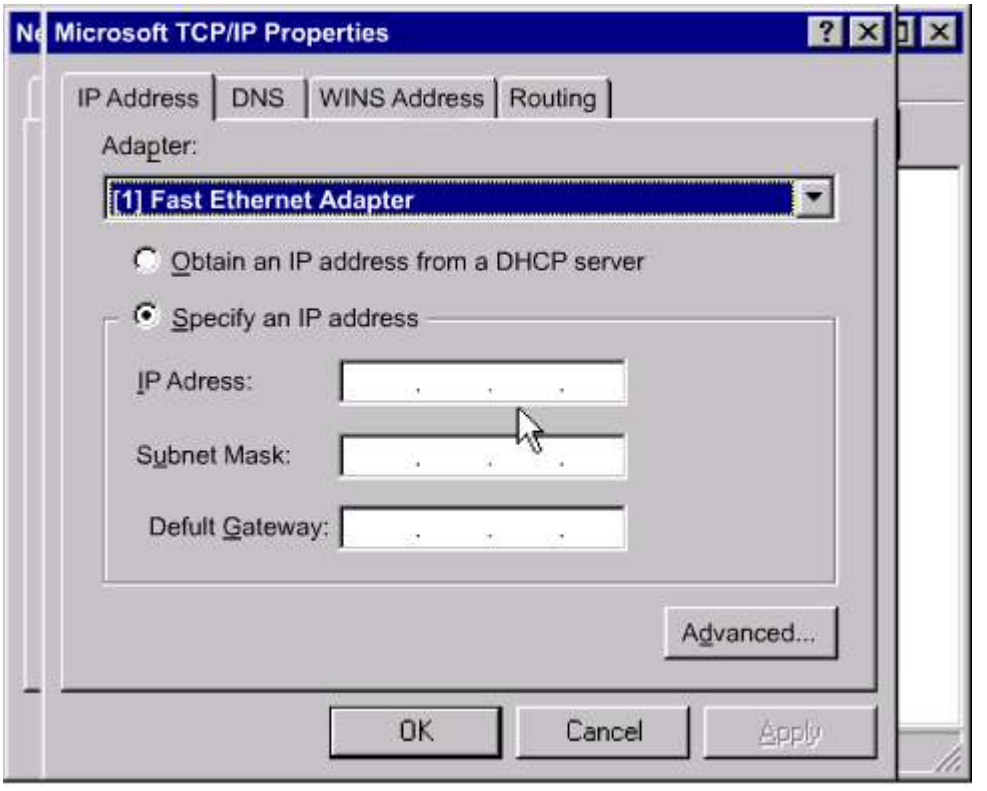
9.3 Obtention d'une adresse IP

9.3.2 Attribution statique d'une adresse IP

Cette page explique le concept d'attribution statique.

L'attribution statique convient particulièrement aux réseaux de petite taille qui subissent peu de changements. L'administrateur système effectue manuellement les opérations d'affectation et de suivi des adresses IP pour chaque ordinateur, imprimante ou serveur de l'intranet. 1


Control Panel
File Edit View Help
Control Panel
Accessibility Options
Add/Remove Programs
Console
Date/Time
Devices
Display
Find Fast
Fonts
Keyboard
Modems
Mouse
Multimedia
Network
PC Card (PCMCIA)
Ports
Printers
Regional Settings
SCSI Adapters
Server
Services
Sounds
System
Tape Devices
Telephony
UPS
23 objects(s)
Network
Identification
Services
Protocols
Adapters
Bindings
Network Protocols:
Apple Talk Protocol
NetBEUI Protocol
TCP/IP Protocol
Add...
Remove
Properties...
Update
Description:
Transport Control Protocol/Internet Protocol. The defult wide area network protocol that provides communication across diverse interconnected networks.
Ok
Cancel

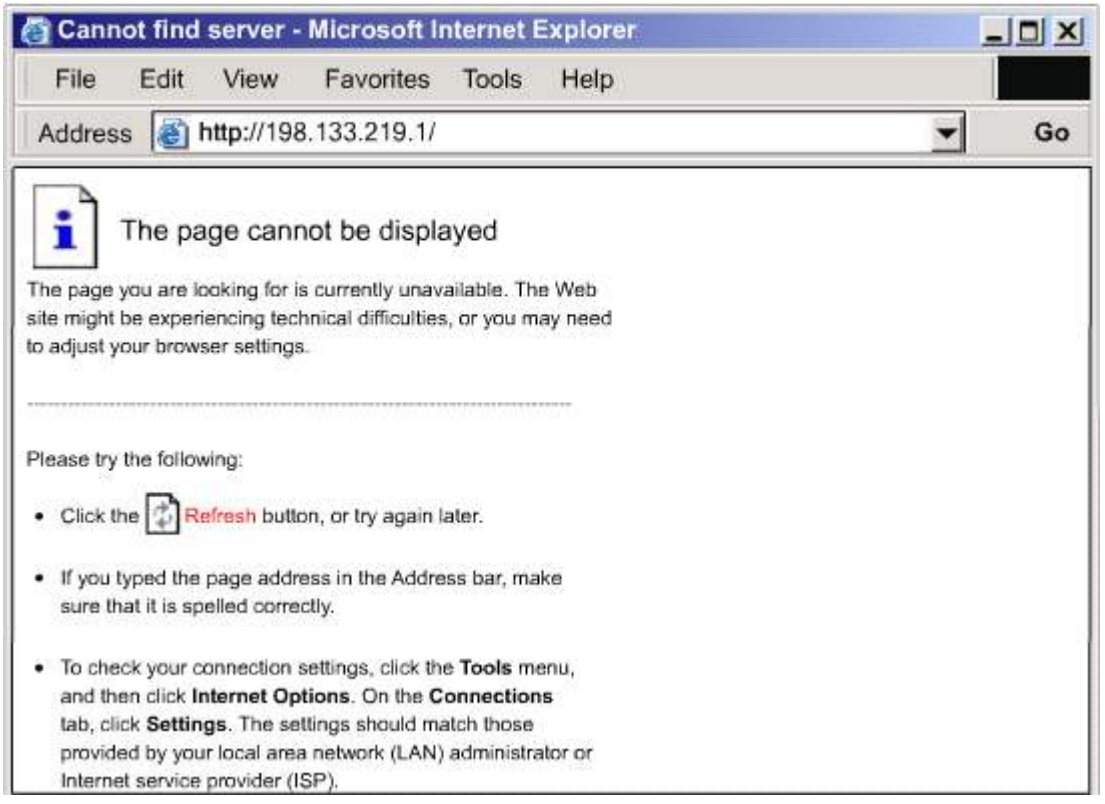


La tenue d'archives est essentielle pour prévenir les conflits d'adresses IP. Toutefois, cette technique n'est possible que dans le cas où peu d'équipements sont connectés au réseau.

Les serveurs doivent recevoir une adresse IP statique de sorte que les stations de travail et les autres équipements puissent toujours accéder aux services requis. 2


Academy Connection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://cisco.netacad.net/public/index.html
Go
Cisco Systems
Contacts & Feedback | Site Help
Academy Connection Home
GO
ACADEMY CONNECTION
Home
Networking Academy
Global Learning Network
Workforce Development
Digital Divide
Newsroom
ACADEMY CONNECTION
Welcome to the Cisco Networking Academy Program web site. Our comprehensive, global e-learning program offers students an opportunity to pursue IT curricula through online instructor-led training and hands-on laboratory exercises. As a result, students can apply classroom learnings to actual technology challenges, which ultimately prepares tomorrow's workforce for life-long learning opportunities.
Search
Search All Cisco.com
Toolkit:
Academy Users Login
Instructors: CCNA | CCNP |
New Curriculum
>> Forgot Username/Password?
>> Initial Registration
>> Get a Serial Number
Students: Student Login
>> Login help
Alumni Connection
Academy Locator
Find an Academy near you.
International Related Sites
Asia Pacific | Canada | EMEA | Japan | Latin America
News and Events
Cisco Networking Academy Program
Networking Academy Program Overview
The Cisco Networking Academy Program is a comprehensive program designed to teach students Internet technology skills.
Global Learning Network
GLN is an AVVID-based comprehensive e-learning solution proven in the Academy Program.


Cisco Systems, Inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://198.133.219.25/
Go
Cisco Systems
Home | Log In | Register | Contacts & Feedback | Site Help
Select an Area
GO
ACADEMY CONNECTION
Cisco Systems is the worldwide leader in networking for the Internet
Business Strategies & Solutions
Learn about trends, strategies, and solutions that can help solve critical business problems, optimize businesses, and enable business productivity.
Networking Solutions & Provisioned Services
Discover how Cisco networking designs, products, and solutions can provide the quality of service, availability, and security that today's Internet businesses require.
Products & Services
Learn about products and services available from Cisco, and find information on product specifications, documentation, and troubleshooting.
Technologies
Research the technologies that support your network infrastructure. Find technical details about protocols and industry standards.
Ordering
Create, place, and manage orders for Cisco products and services. Access ordering information and other support materials.
Search
Search All Cisco.com
Toolkit:
Log In
Log In here to gain access to additional tools and content.
- New User? Register now.
- Forgot your password? Click here.
Click Here
Cisco Systems
2002 Annual Report
Take the Cisco.com
Site Tour
Access former
Web site


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://198.133.219.1/
Go
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
Please try the following:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).

Imaginez combien il serait complexe d'appeler une entreprise qui change quotidiennement de numéro de téléphone.

Les autres équipements nécessitant des adresses IP statiques sont les imprimantes réseau, les serveurs d'applications et les routeurs.

La page suivante présente le protocole RARP (*Reverse Address Resolution Protocol*).

9.3 Obtention d'une adresse IP

9.3.3 Attribution d'une adresse IP à l'aide du protocole RARP

Cette page traite de l'attribution d'adresses par l'intermédiaire du protocole RARP.

Le protocole RARP associe des adresses MAC connues à des adresses IP. Cette association permet à certains équipements d'encapsuler les données avant de les envoyer sur le réseau. Un équipement réseau, tel qu'une station de travail sans disque dur local, peut connaître son adresse MAC mais ignorer son adresse IP. Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP. Les équipements utilisant le protocole de résolution inverse d'adresses requièrent un serveur RARP pour répondre aux requêtes de ce protocole.

Examinons l'exemple d'un équipement source qui souhaite envoyer des données à un autre équipement. L'équipement source connaît sa propre adresse MAC, mais il ne trouve pas son adresse IP dans la table ARP. Pour que l'équipement de destination puisse récupérer les données, les transférer aux couches supérieures du modèle OSI et répondre à l'équipement source, ce dernier doit indiquer son adresse MAC et son adresse IP. L'équipement source lance alors un processus appelé «requête RARP». Cette requête permet d'aider le matériel source à détecter sa propre adresse IP. Les requêtes RARP sont diffusées sur le LAN et c'est le serveur RARP, habituellement un routeur, qui y répond.

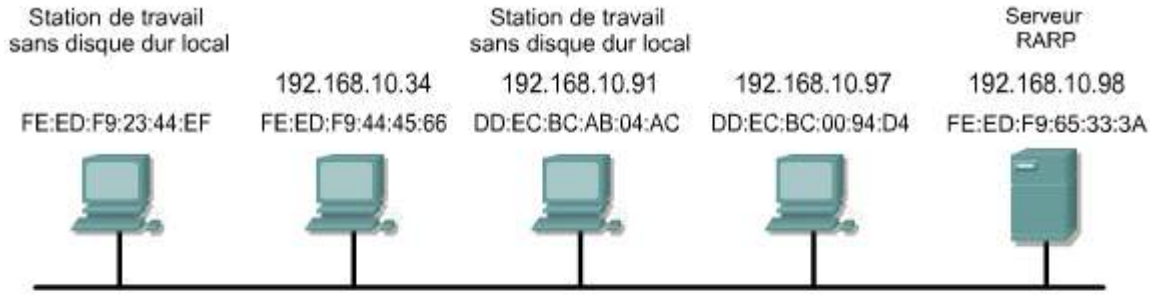
Le protocole de résolution inverse d'adresses utilise le même format de paquet que le protocole ARP. Cependant, dans une requête RARP, les en-têtes MAC et le code de fonctionnement sont différents de ceux d'une requête ARP. 1 2

0 - 15 bits		16 - 31 bits
Type de matériel		Type de protocole
HLen (1 octet)	PLen (1 octet)	Opération
AM expéditeur (octets 1 - 4)		
AM expéditeur (octets 5 - 6)		AP expéditeur (octets 1 - 2)
AP expéditeur (octets 3 - 4)		AM cible (octets 1 - 2)
AM cible (octets 3 - 6)		
AP cible (octets 1 - 4)		

Structure de l'en-tête RARP

Champ	Description
Type de matériel	Spécifie un type d'interface matérielle pour lequel l'expéditeur attend une réponse.
Type de protocole	Spécifie le type d'adresse de protocole de haut niveau fourni par l'expéditeur.
HLen	Longueur de l'adresse matérielle.
PLen	Longueur de l'adresse de protocole.
Opération	Les valeurs sont les suivantes : 1 Requête ARP 2 Réponse ARP 3 Requête RARP 4 Réponse RARP 5 Requête RARP dynamique 6 Réponse RARP dynamique 7 Erreur RARP dynamique 8 Requête InARP 9 Réponse InARP
Adresse matérielle (AM) de l'expéditeur	Longueur en octets HLen.
Adresse de protocole (AP) de l'expéditeur	Longueur en octets PLen.
Adresse matérielle (AM) de la cible	Longueur en octets HLen.
Adresse de protocole (AP) de la cible	Longueur en octets PLen.

La structure du paquet RARP contient des champs pour les adresses MAC des équipements d'origine et de destination. Le champ de l'adresse IP d'origine est vide. Le message de broadcast est envoyé à tous les équipements du réseau. Les figures 4, 5



En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF
Champ Type	FF:FF:FF:FF		
0X8035 (Ethernet)	non défini		

Fenêtre contextuelle (pop up)

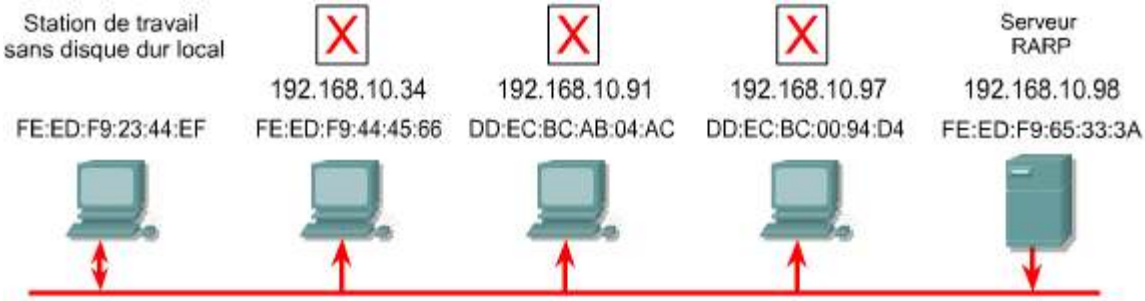
L'ordinateur FE:ED:F9:23:44:EF génère une requête RARP.



En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF
Champ Type	FF:FF:FF:FF		
0X8035 (Ethernet)	non défini		

Fenêtre contextuelle (pop up)

L'ordinateur FE:ED:F9:23:44:EF transmet une requête RARP.



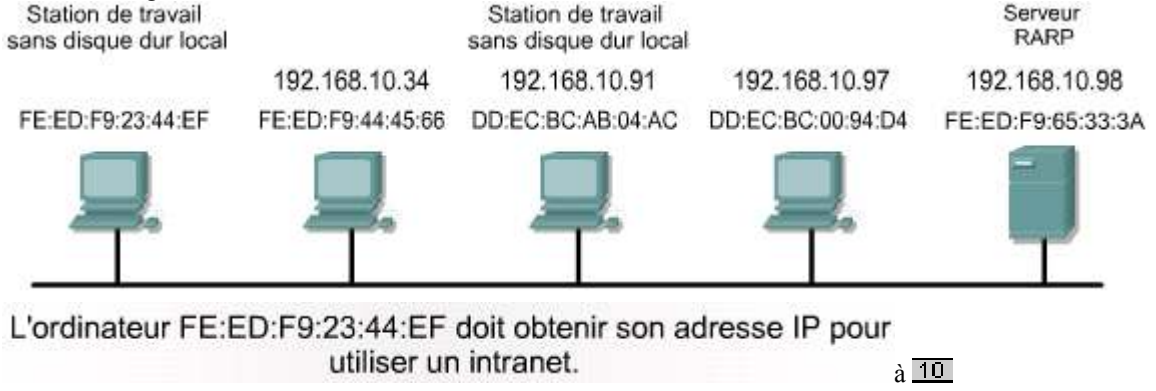
En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF
Champ Type	FF:FF:FF:FF		
0X8035 (Ethernet)	non défini		

Fenêtre contextuelle (pop up)

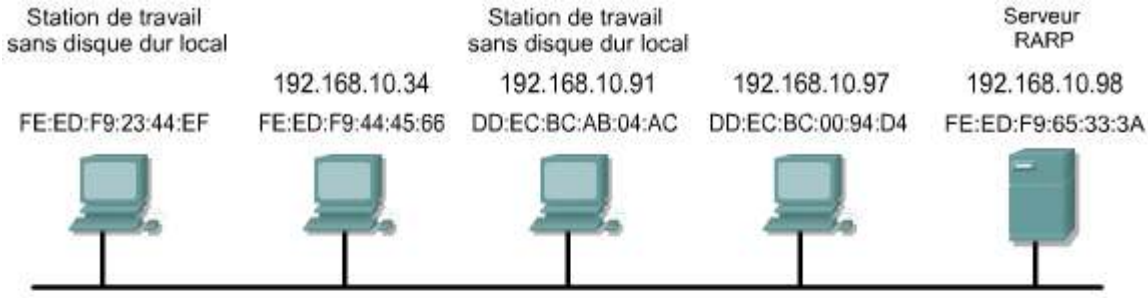
Tous les ordinateurs transmettent le paquet à la couche réseau. Si les numéros IP ne correspondent pas, le paquet est supprimé, sauf sur le serveur RARP, qui détecte le champ de requête RARP.

et 6

illustrent l'adresse MAC de destination sous la forme FF:FF:FF:FF:FF:FF. Les stations de travail exécutant le protocole de résolution inverse d'adresses comportent des codes en mémoire ROM qui déclenchent le processus RARP. Les figures 3



à 10



En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	4
FE:ED:F9:65:33:3A	FE:ED:F9:23		
Adresse MAC de destination	44:EF		192.168
FE:ED:F9:23:44:EF	10.36		FE:ED
Champ Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Fenêtre contextuelle (pop up)

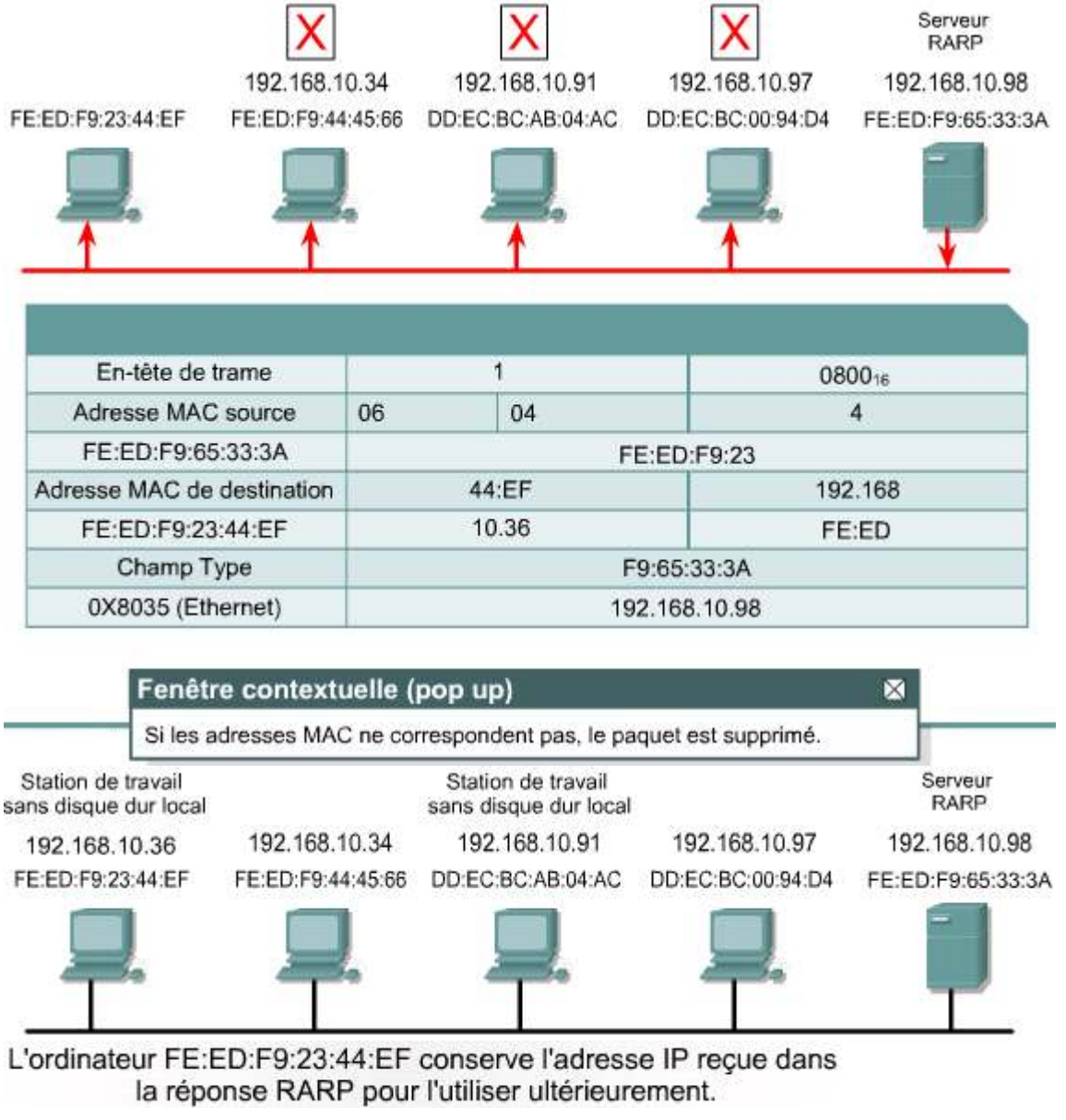
Le serveur RARP crée un message de réponse RARP pour le client à l'origine de le client à l'origine



En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	4
FE:ED:F9:65:33:3A	FE:ED:F9:23		
Adresse MAC de destination	44:EF		192.168
FE:ED:F9:23:44:EF	10.36		FE:ED
Champ Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

Fenêtre contextuelle (pop up)

Tous les ordinateurs copient la trame et l'examinent.



indiquent avec précision le processus RARP.

La page suivante traite du protocole BOOTP (*Bootstrap Protocol*).

9.3 Obtention d'une adresse IP

9.3.4 Attribution d'une adresse IP à l'aide du protocole BOOTP

Cette page présente le protocole BOOTP.

Le protocole BOOTP fonctionne dans un environnement client-serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP. [1] [2]

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Non utilisé	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (64 octets)			
Structure des messages BOOTP			

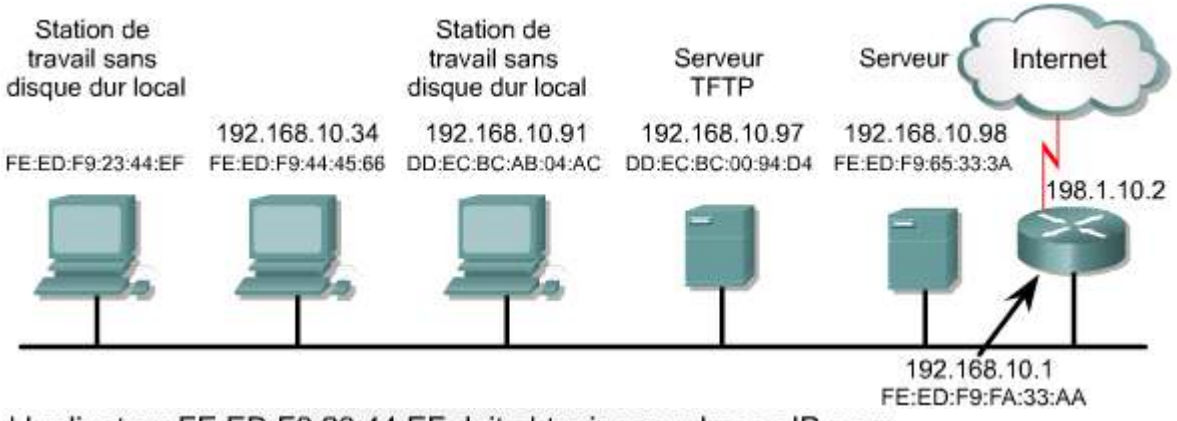
Champ	Description
Op	Code de fonctionnement des messages. Les messages peuvent être de type BOOTREQUEST ou BOOTREPLY.
Htype	Type d'adresse matérielle
HLen	Longueur de l'adresse matérielle
Hops	Le client ajoute un zéro ; ce champ est utilisé par le serveur BOOTP pour envoyer des requêtes à un autre réseau.
Xid	ID de la transaction
Secs	Secondes écoulées depuis le début du processus de renouvellement ou de l'acquisition de l'adresse par le client.
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (client)
Siaddr	Adresse IP du serveur suivant à utiliser dans le bootstrap
Giaddr	Adresse IP de l'agent de relais utilisée pour l'amorçage via un agent de relais
Chaddr	Adresse matérielle du client
Server Host Name	Spécifie le serveur qui doit fournir les informations BOOTP.
Boot File Name	Permet d'utiliser plusieurs fichiers de démarrage ; les hôtes peuvent alors exécuter différents systèmes d'exploitation.
Vendor Specific Area	Contient des informations facultatives propres au fournisseur qui peuvent être transmises à l'hôte.

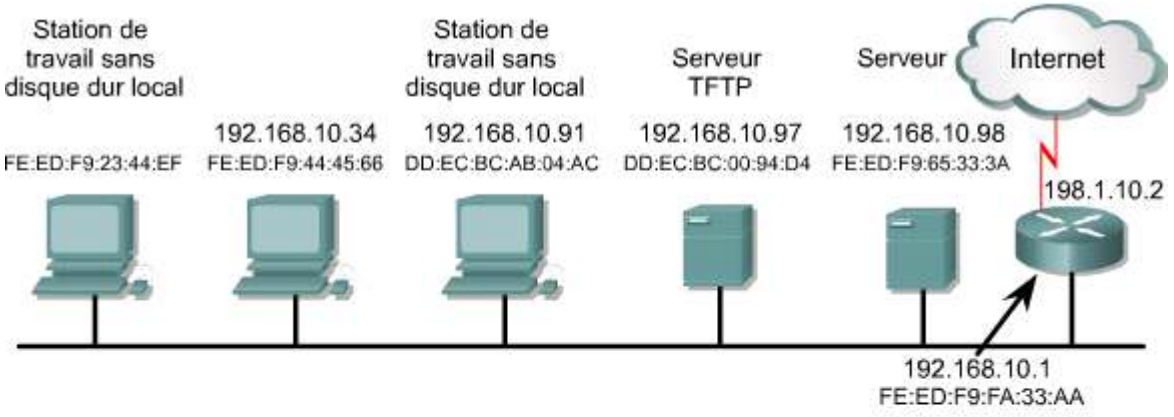
Contrairement au protocole RARP, les paquets BOOTP peuvent contenir l'adresse IP, l'adresse du routeur, l'adresse du serveur ainsi que des informations spécifiques du fournisseur.

L'un des problèmes du protocole BOOTP est de ne pas avoir été conçu pour l'attribution dynamique d'adresses. Il permet à un administrateur réseau de créer un fichier de configuration qui définit les paramètres de chaque équipement. L'administrateur doit ajouter les hôtes et tenir à jour la base de données BOOTP. Bien que les adresses soient attribuées de manière dynamique, il existe une relation biunivoque entre le nombre d'adresses IP et le nombre d'hôtes. Autrement dit, à chaque hôte du réseau doit correspondre un profil BOOTP comportant

une adresse IP. Deux profils ne peuvent pas partager une même adresse IP. Ces profils pourraient être utilisés simultanément, ce qui signifierait que deux hôtes disposent d'une même adresse IP.

Un équipement utilise le protocole BOOTP au démarrage pour obtenir une adresse IP. BOOTP utilise la couche UDP pour transporter les messages. Le message UDP est encapsulé dans un paquet IP. Un ordinateur utilise le protocole BOOTP pour envoyer un paquet IP de broadcast en utilisant une adresse IP de destination constituée de tous les 1 binaires (255.255.255.255 en notation décimale séparée par des points). Un serveur BOOTP reçoit le message de broadcast, puis en envoie un à son tour. Le client reçoit une trame et vérifie l'adresse MAC. Si le client trouve sa propre adresse MAC dans le champ d'adresse de destination et une adresse de broadcast dans le champ de destination IP, il enregistre et stocke l'adresse IP ainsi que toutes les informations fournies dans le message de réponse BOOTP. Les figures 3 à 10 indiquent avec précision le processus BOOTP.



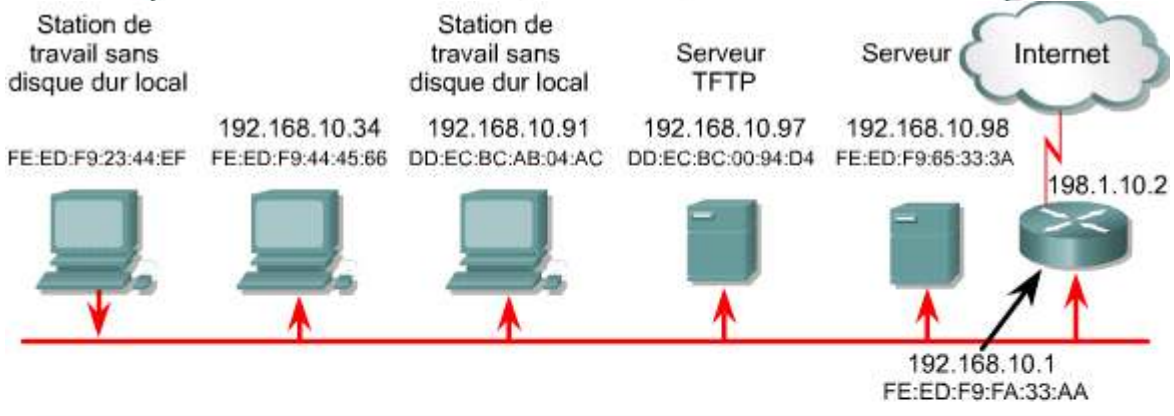


En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Copyright sur l'in

Fenêtre contextuelle (pop up)

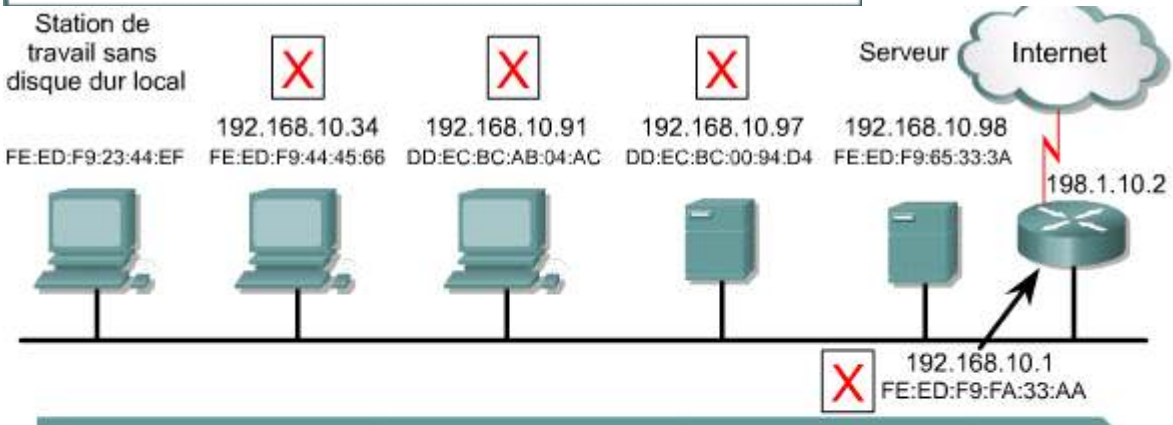
L'ordinateur FE:ED:F9:23:44:EF génère une requête BOOTP.



En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

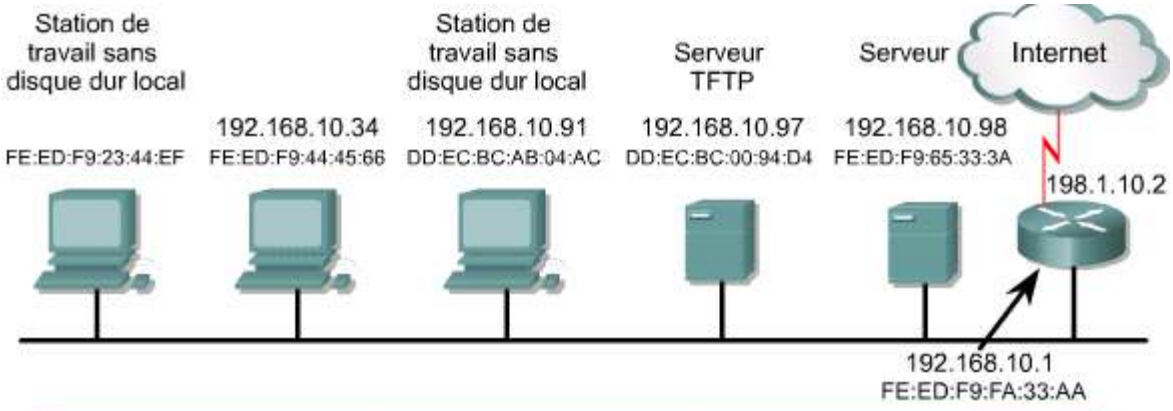
La station de travail FE:ED:F9:23:44:EF encapsule la requête dans l'en-tête d'un paquet. L'en-tête contient une adresse IP source inconnue et une adresse IP de destination de broadcast. Pour l'en-tête de la trame, la station de travail utilise son adresse MAC en tant que source et un broadcast pour la destination car elle ne connaît pas l'adresse du serveur BOOTP. La station de travail transmet alors une trame de requête BOOTP.



En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

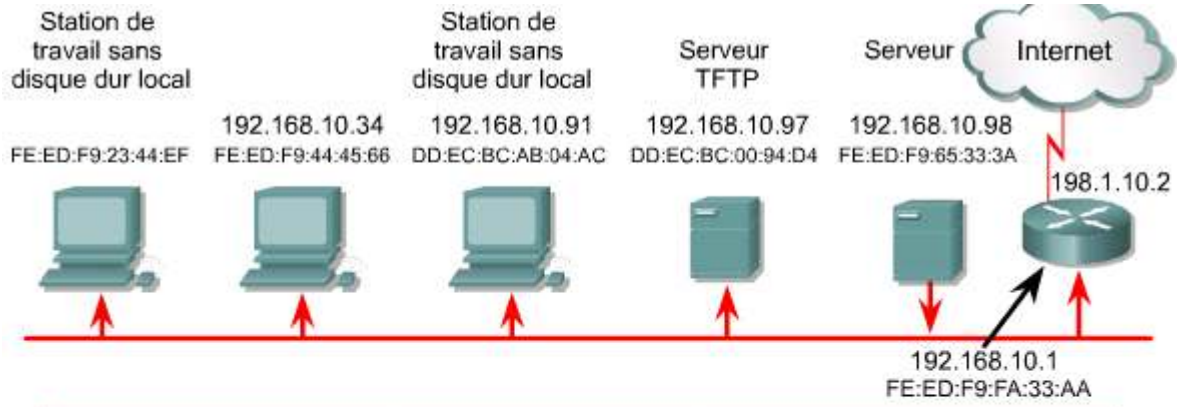
Toutes les unités extraient une copie de la trame, détectent une adresse MAC de destination de broadcast, retirent l'en-tête et transmettent le paquet à la couche réseau. Les unités détectent que l'adresse de destination IP est une adresse IP de broadcast, retirent l'en-tête du paquet et transmettent les données de la réponse à la couche transport. Toutes les unités détectent le champ de requête BOOTP en tant que requête BOOTP. Elle est alors ignorée de toutes les unités, à l'exception du serveur BOOTP.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

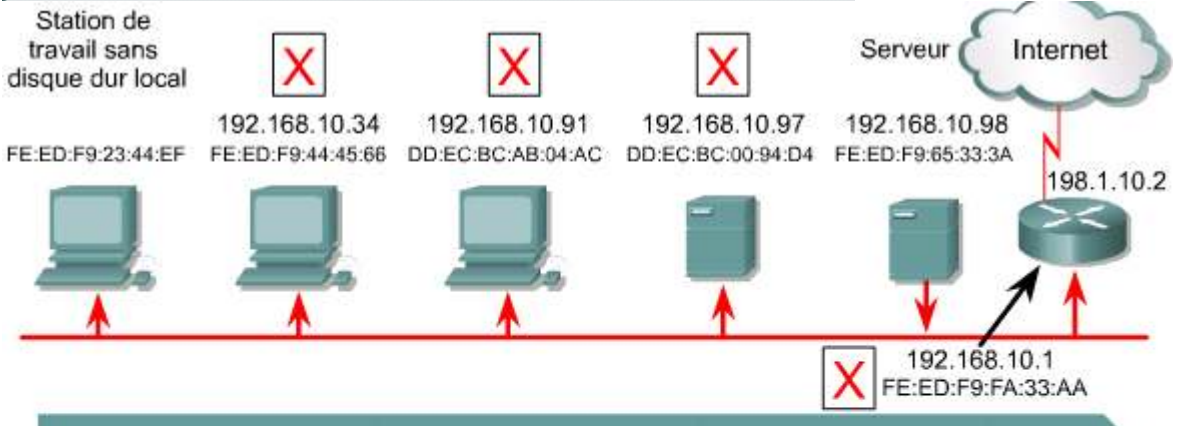
À partir de sa base de données, le serveur prépare une réponse BOOTP destinée à l'unité qui est à l'origine de la demande. Cette réponse inclut l'adresse IP du client, l'adresse du serveur TFTP et l'adresse de la passerelle par défaut (les autres champs sont omis pour cet exemple). Dans l'en-tête de la trame, les adresses source et de destination sont inversées. Dans l'en-tête du paquet, le serveur BOOTP place son adresse IP dans le champ source et une adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse BOOTP au niveau de la couche transport en vue de son traitement. Seul un broadcast sera acheminé puisque le client ne connaît pas son adresse IP.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

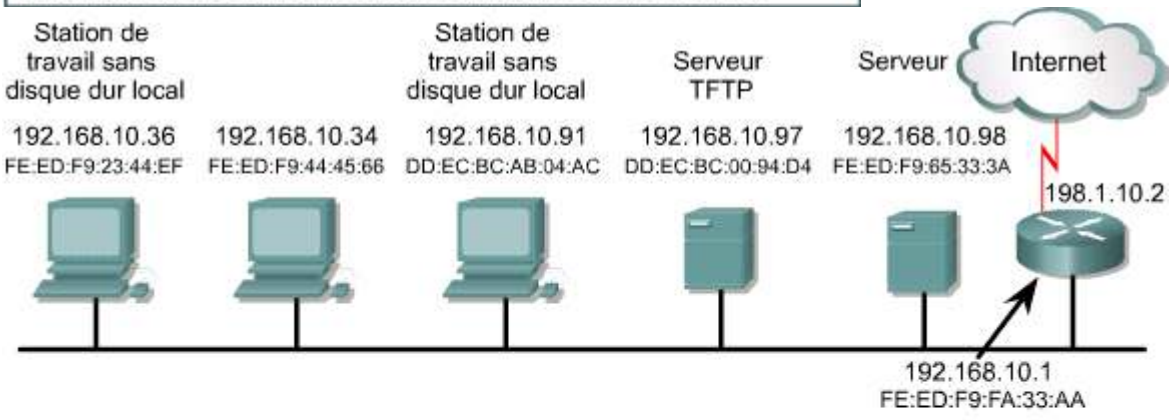
Le serveur BOOTP renvoie alors la trame de la réponse BOOTP à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur BOOTP sont alors stockées dans la table ARP de la station de travail sans disque dur local. L'en-tête de la trame est retiré et ignoré.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

Fenêtre contextuelle (pop up)

L'adresse IP de destination du paquet étant un broadcast, l'en-tête du paquet est retiré et les données de la réponse BOOTP sont transmises à la couche transport, dans laquelle les données du champ OP indiquent qu'il s'agit d'une réponse BOOTP. Les données de la réponse sont stockées dans les emplacements de mémoire appropriés de la station de travail. La station de travail a maintenant accès au serveur TFTP, pour télécharger d'autres systèmes d'exploitation, et à la passerelle par défaut. Elle dispose également de sa propre adresse IP. Elle peut donc être utilisée avec le réseau et Internet.

La page suivante traite du protocole DHCP (*Dynamic Host Configuration Protocol*).

9.3 Obtention d'une adresse IP

9.3.5 Gestion des adresses IP à l'aide du protocole DHCP

Cette page décrit les caractéristiques et les avantages du protocole DHCP.

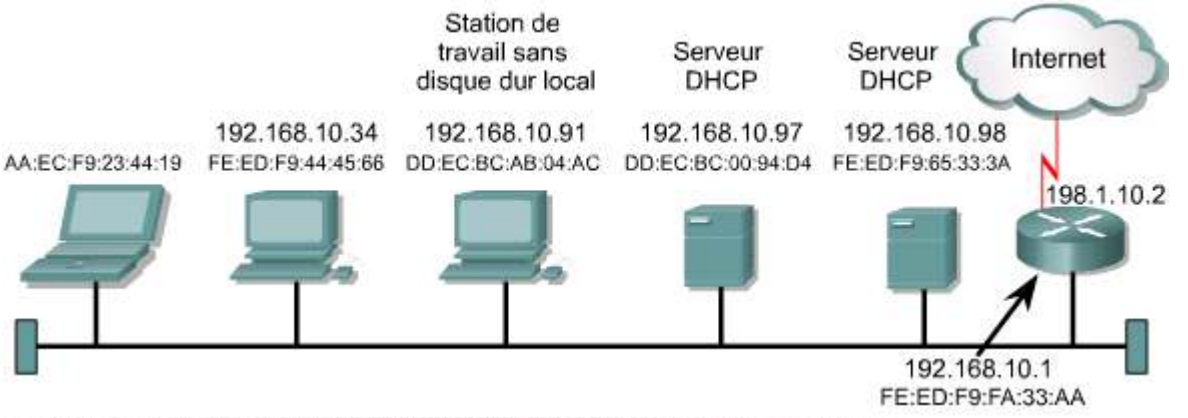
Le protocole DHCP a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de manière dynamique sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie sur un serveur DHCP. Lorsque les ordinateurs se connectent, ils communiquent avec le serveur DHCP et demandent une adresse. Le serveur DHCP choisit une adresse et l'affecte à l'ordinateur hôte. Grâce au protocole DHCP, la configuration réseau tout entière d'un ordinateur peut être obtenue dans un seul message. 1 2

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Indicateurs (2 octets)	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (variable)			
Structure des messages DHCP			

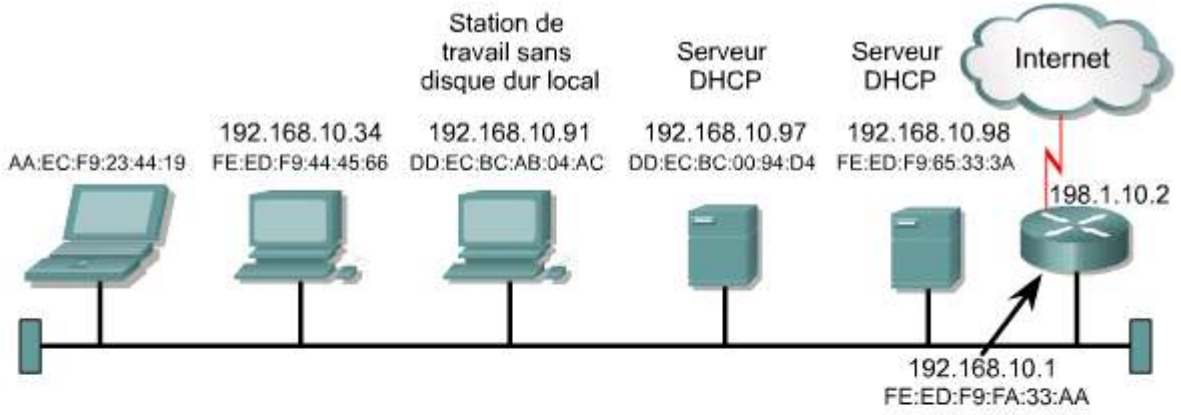
Op	Les messages des codes de fonctionnement des messages peuvent être de type BOOTREQUEST ou BOOTREPLY.
Htype	Type d'adresse matérielle
Hlen	Longueur de l'adresse matérielle
Hops	Le client ajoute un zéro ; ce champ est utilisé par le serveur BOOTP pour envoyer des requêtes à un autre réseau.
Xid	ID de la transaction
Secs	Secondes écoulées depuis le début du processus de renouvellement ou de l'acquisition de l'adresse par le client.
Indicateurs	Indicateurs
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (client)
Siaddr	Adresse IP du serveur suivant à utiliser dans le bootstrap
Giaddr	Adresse IP de l'agent de relais utilisée pour l'amorçage via un
Chaddr	Adresse matérielle du client
Server Host Name	Spécifie le serveur qui doit fournir les informations BOOTP.
Boot File Name	Permet d'utiliser plusieurs fichiers de démarrage ; les hôtes peuvent alors exécuter différents systèmes d'exploitation.
Vendor Specific Area	Contient des informations facultatives propres au fournisseur qui peuvent être transmises à l'hôte.

Cela comprend les données fournies par le message BOOTP, plus une adresse IP allouée et un masque de sous-réseau.

Le protocole DHCP dispose d'un avantage majeur sur le protocole BOOTP, car il permet aux utilisateurs d'être mobiles. Les utilisateurs peuvent changer de connexion réseau d'un emplacement à l'autre, et ce en toute liberté. Il n'est plus nécessaire d'utiliser un profil fixe pour chaque équipement relié au réseau, comme cela était le cas avec le système BOOTP. Cette évolution revêt une importance particulière dans la mesure où le protocole DHCP peut octroyer une adresse IP à un équipement, puis utiliser cette même adresse pour un autre utilisateur lorsque le premier ne s'en sert plus. Autrement dit, le protocole DHCP offre une relation «un à plusieurs» pour les adresses IP. De plus, une adresse est disponible pour quiconque se connectant au réseau. Les figures 3 à 17



L'ordinateur portable AA:EC:F9:23:44:19 doit obtenir une adresse IP pour les opérations effectuées sur l'intranet et Internet.

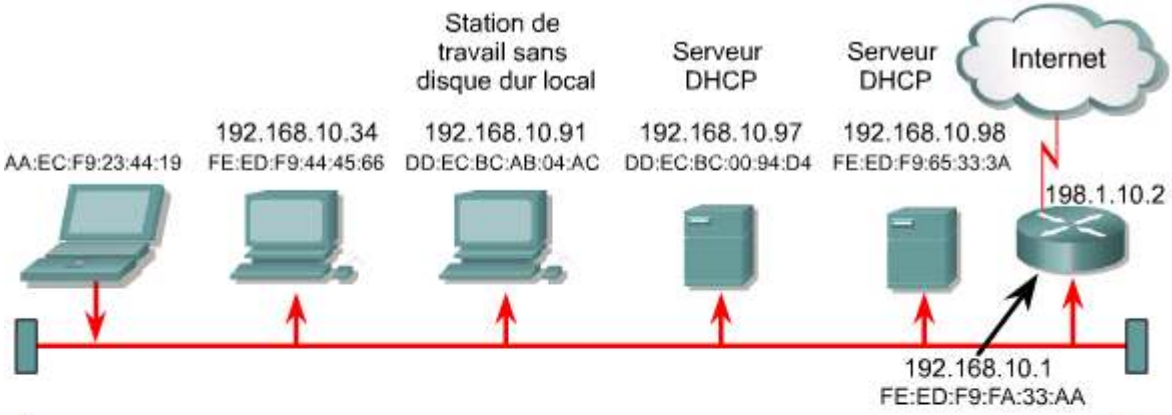


En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	221				
AA:EC:F9:23:44:19	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Type de champ		0				
0X8035 (Ethernet)		AA:EC:F9:23:44:19				
		53	1	2		

Copyright sur l'in

Fenêtre contextuelle (pop up)

L'ordinateur portable AA:EC:F9:23:44:19 génère une requête DHCP.

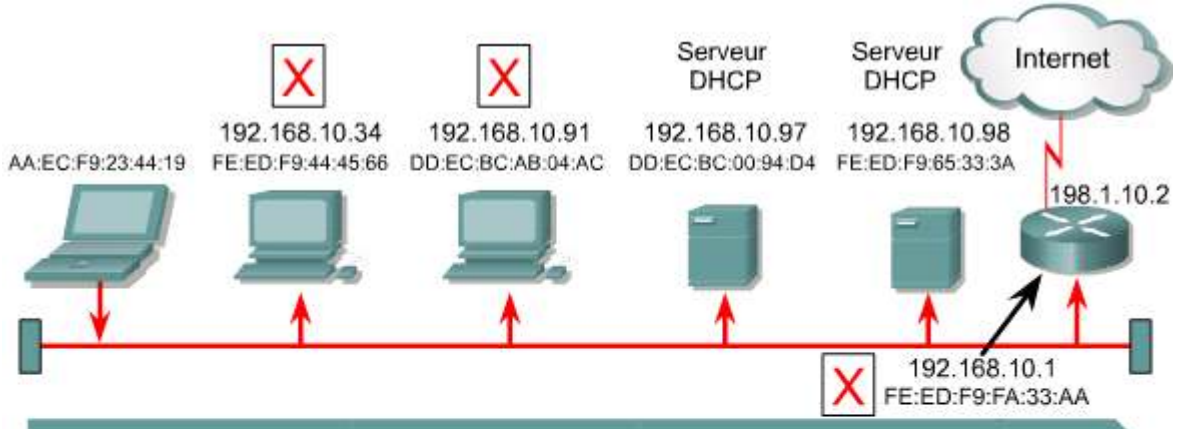


En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	221				
AA:EC:F9:23:44:19	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Type de champ		0				
0X8035 (Ethernet)		0				
		AA:EC:F9:23:44:19				
		53	1	2		

Copyright sur l'in

Fenêtre contextuelle (pop up)

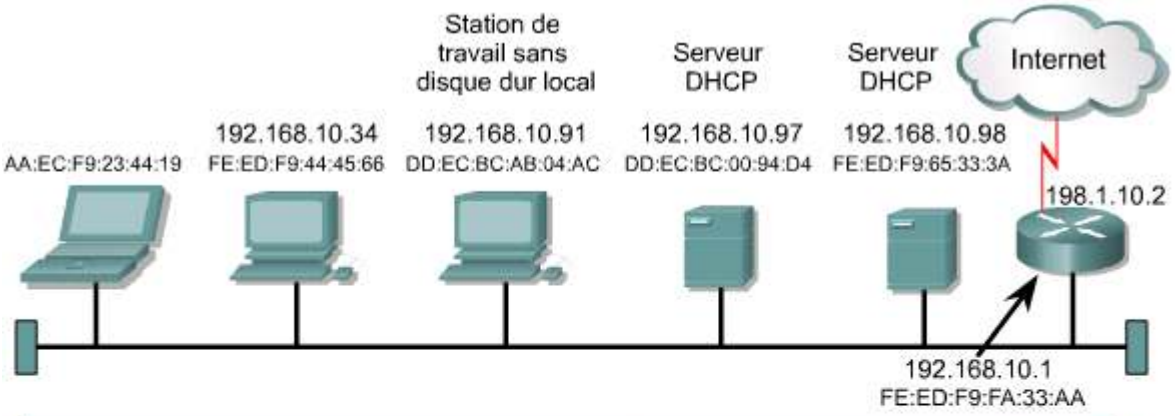
La requête DHCP est transmise par l'ordinateur portable.



En-tête de trame	En-tête du paquet	1	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	221				
AA:EC:F9:23:44:19	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	255.255.255.255	0				
Type de champ		0				
0X8035 (Ethernet)		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

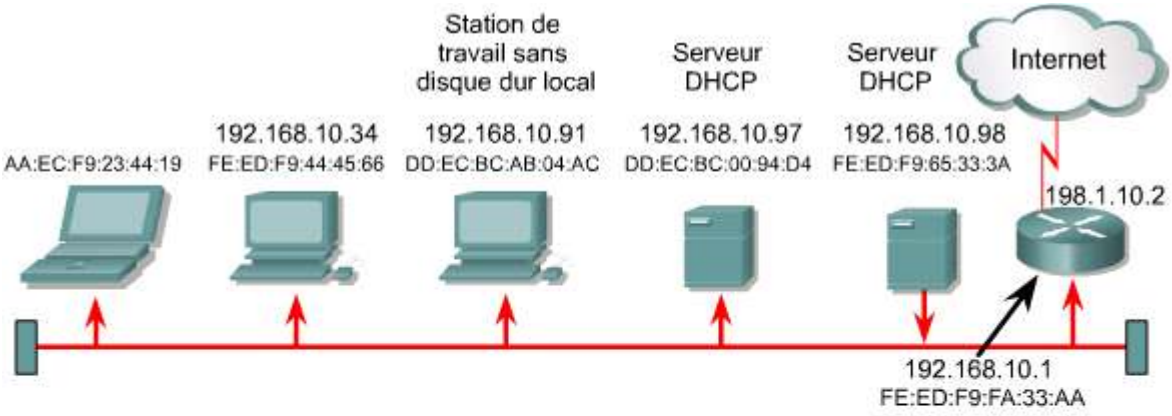
Toutes les unités extraient une copie de la trame, détectent une adresse MAC de destination de broadcast, retirent l'en-tête et transmettent le paquet à la couche réseau. Les unités détectent que l'adresse de destination IP est une adresse IP de broadcast, retirent l'en-tête du paquet et transmettent les données de la réponse à la couche transport. Toutes les unités détectent le champ de requête DHCP en tant que requête DHCP. Elle est alors ignorée par toutes les unités, à l'exception des serveurs DHCP.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FE:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

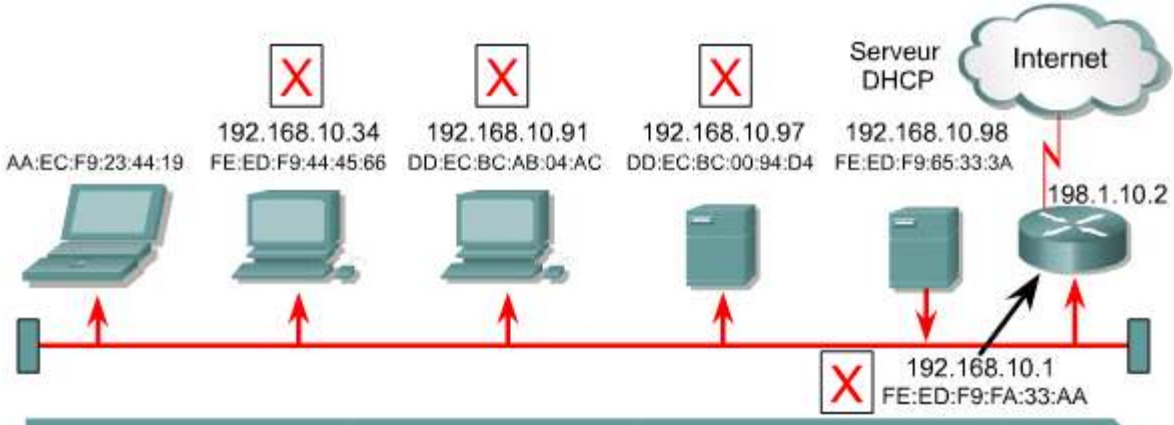
Le serveur prépare une offre DHCP à renvoyer à l'unité qui est à l'origine de la demande. Elle inclut l'adresse IP du client, l'adresse du serveur DHCP et l'adresse de la passerelle par défaut. Dans l'en-tête de la trame, les adresses source et de destination sont inversées. Dans l'en-tête du paquet, le serveur DHCP place son adresse IP dans le champ source et une adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse DHCP au niveau de la couche transport en vue de son traitement. Seul un broadcast sera acheminé puisque le client ne connaît pas son adresse IP.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FE:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

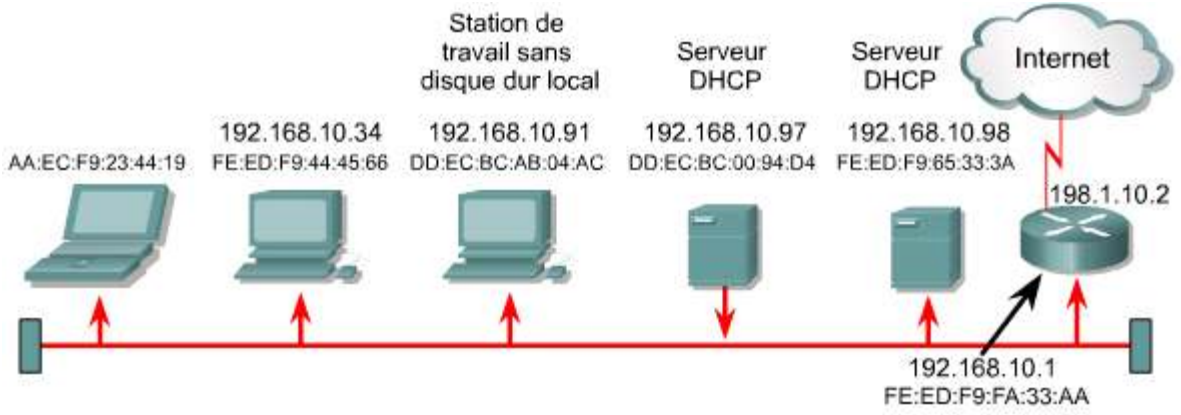
Le serveur DHCP renvoie alors la trame de la réponse DHCP à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FE:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

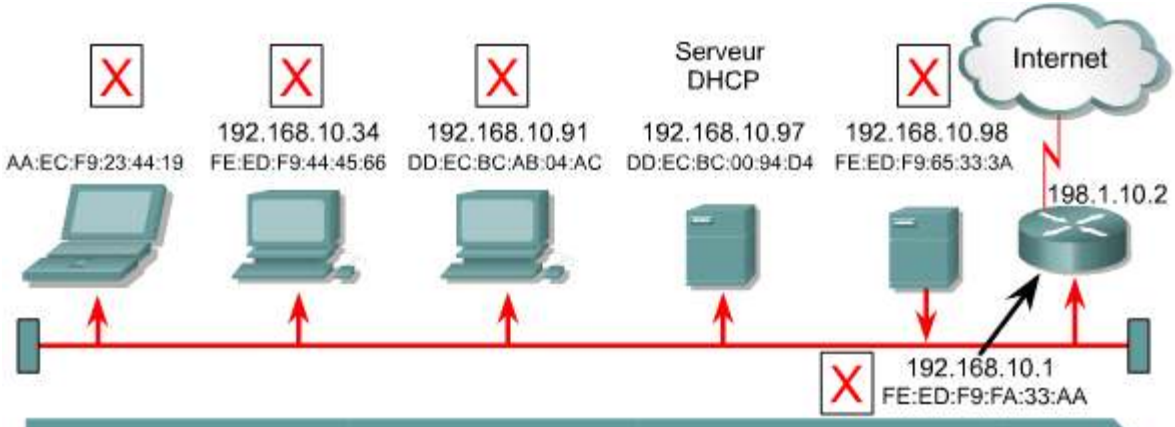
L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
DD:EC:BC:00:94:D4	192.168.10.97	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.90				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

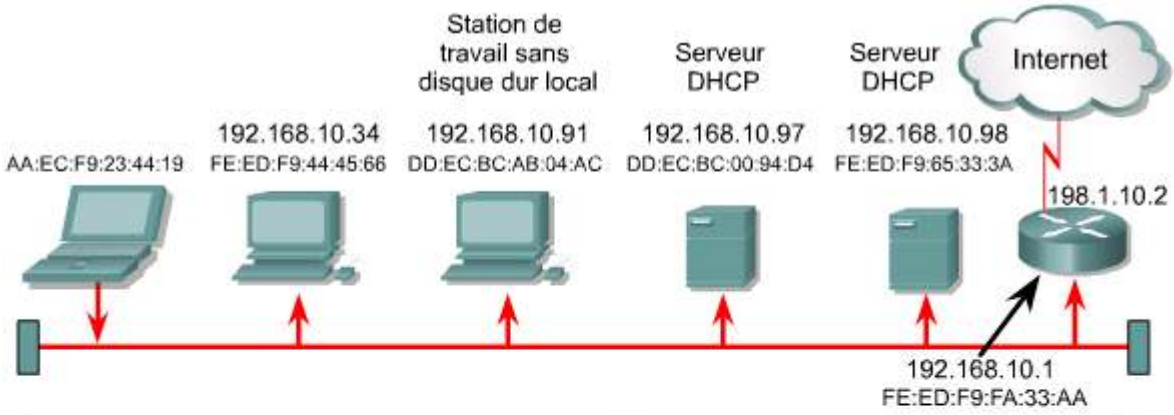
Le deuxième serveur DHCP renvoie alors la trame de la réponse DHCP à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
DD:EC:BC:00:94:D4	192.168.10.97	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.90				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

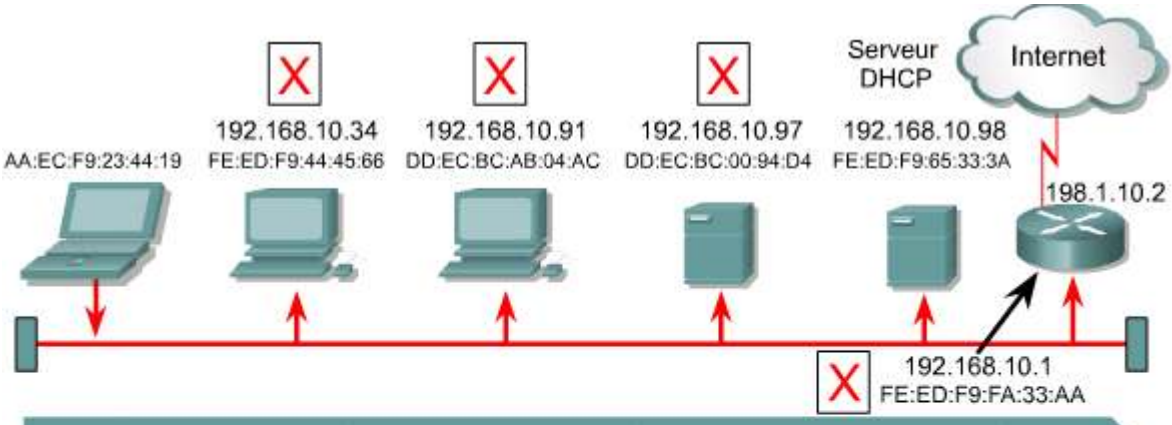
L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC est celle de l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré. L'ordinateur portable ayant déjà reçu une offre DHCP d'un autre serveur, l'offre est ignorée.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FA:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Fenêtre contextuelle (pop up)

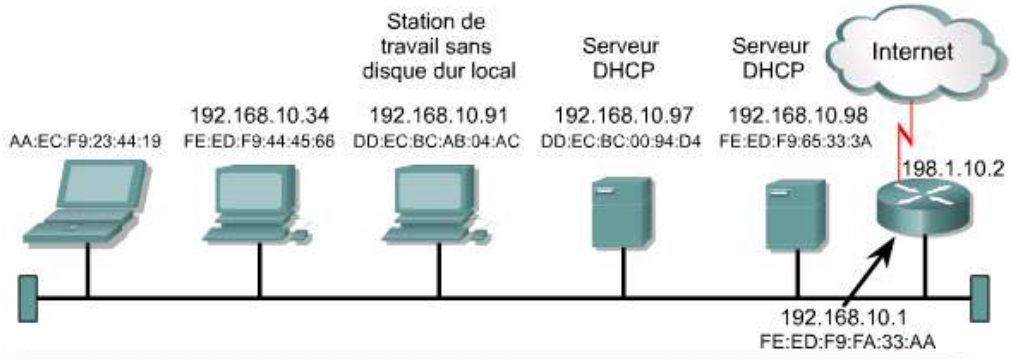
L'ordinateur portable peut maintenant envoyer une requête DHCPREQUEST au serveur DHCP spécifié qui est à l'origine de l'offre acceptée.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FA:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Fenêtre contextuelle (pop up)

Toutes les unités extraient une copie de la trame et comparent la destination MAC avec la leur. En l'absence de correspondance, l'unité ignore la trame.

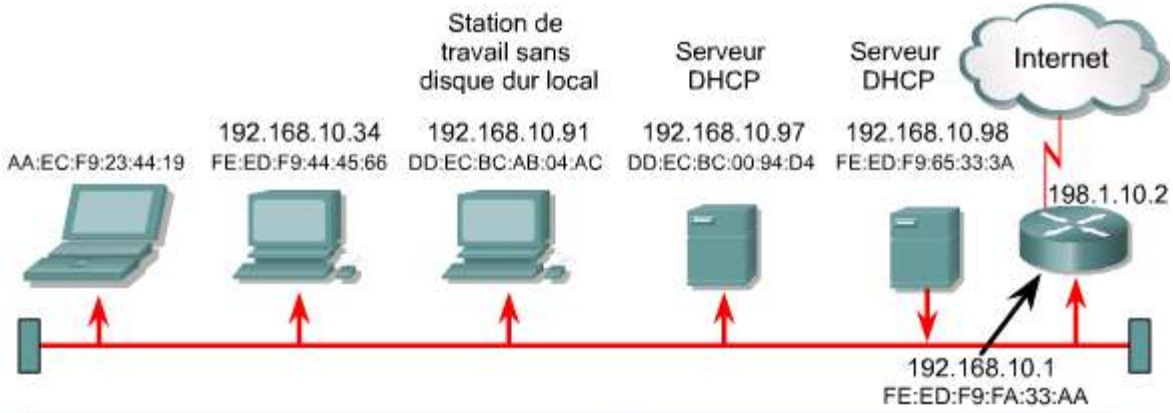


En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FA:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Copyright sur l'

Fenêtre contextuelle (pop up)

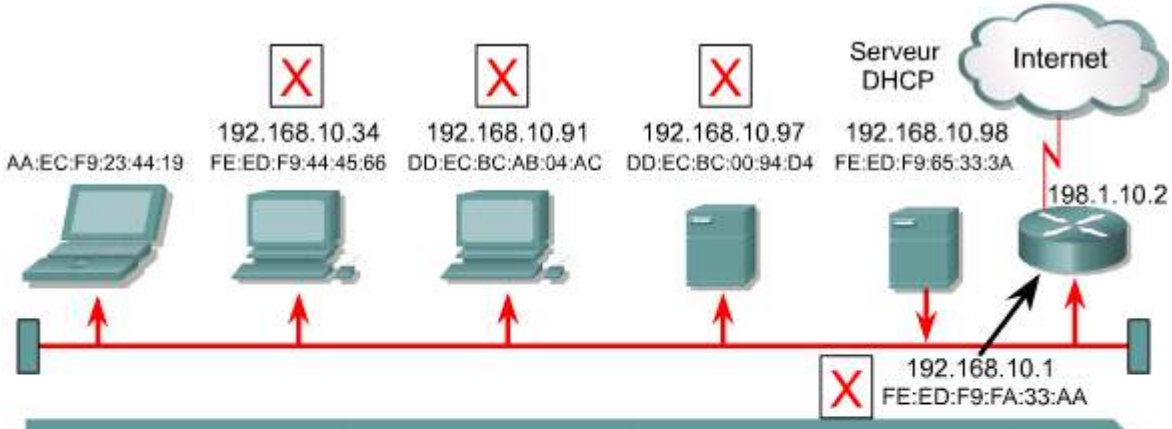
Le serveur DHCP sélectionné crée un DHCPACK.



En-tête de trame	En-tête du paquet	2	1	6	0	Vérification du CRC
Adresse MAC source	Adresse IP source	12				
FA:ED:F9:65:33:3A	192.168.10.98	2		Indicateurs		
Adresse MAC de destination	Adresse IP de destination	0				
AA:EC:F9:23:44:19	255.255.255.255	192.168.10.35				
Type de champ		0				
0X8035 (Ethernet)		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	5		

Fenêtre contextuelle (pop up)

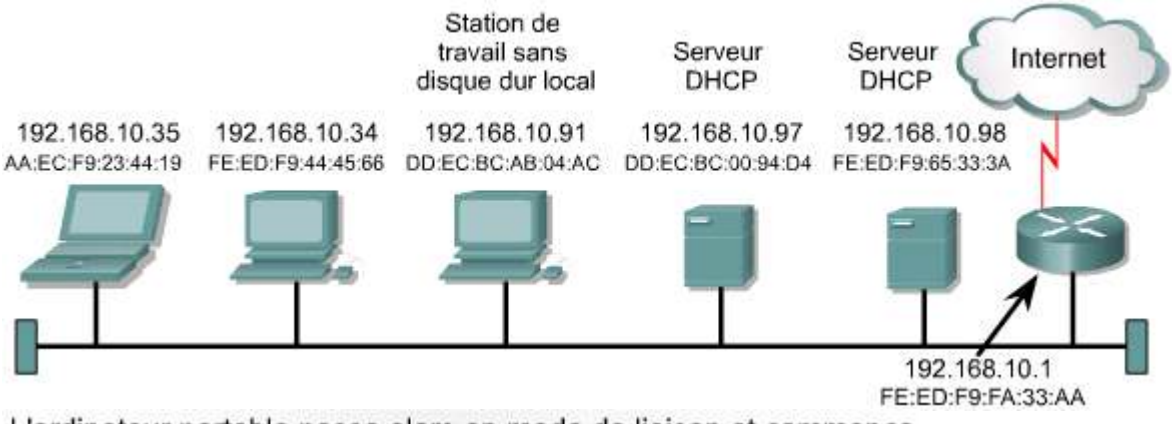
Le serveur DHCP renvoie alors la trame de DHCPACK à l'unité qui est à l'origine de la demande. Toutes les unités extraient le paquet et l'examinent.



En-tête de trame	En-tête du paquet					
Adresse MAC source	Adresse IP source	2	1	6	0	Vérification du CRC
FA:ED:F9:65:33:3A	192.168.10.98	12				
Adresse MAC de destination	Adresse IP de destination	2		Indicateurs		
AA:EC:F9:23:44:19	255.255.255.255	0				
Type de champ		192.168.10.35				
0X8035 (Ethernet)		0				
		192.168.10.1				
		AA:EC:F9:23:44:19				
		53	1	2		

Fenêtre contextuelle (pop up)

L'adresse MAC de destination ne leur correspondant pas et n'étant pas un broadcast, le paquet est ignoré. L'adresse MAC correspond à l'unité client qui est à l'origine de la demande. Les adresses MAC et IP source du serveur DHCP sont alors stockées dans la table ARP de l'ordinateur portable. L'en-tête de la trame est retiré et ignoré.



L'ordinateur portable passe alors en mode de liaison et commence à utiliser l'adresse IP attribuée ainsi que d'autres données transmises avec le message de l'offre DHCP.

indiquent avec précision le processus DHCP.

L'activité de TP vous aidera à configurer un ordinateur réseau en tant que client DHCP.

La page suivante décrit les problèmes les plus fréquemment rencontrés lors de la résolution d'adresses.

Activité de TP

Exercice: Configuration des clients DHCP

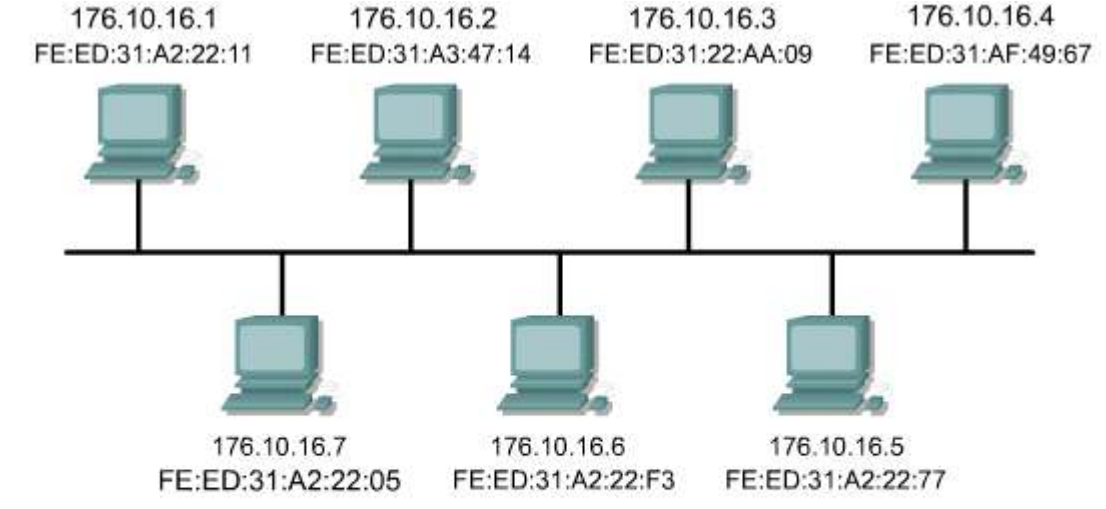
L'objectif de ce TP est de présenter le protocole DHCP (*Dynamic Host Configuration Protocol*) et le processus de configuration d'un ordinateur d'un réseau en tant que client DHCP pour utiliser les services de ce protocole.

9.3 Obtention d'une adresse IP

9.3.6 Problèmes liés à la résolution d'adresses

Cette page présente les problèmes associés à la résolution des adresses.

L'une des principales difficultés liées au réseau est d'arriver à communiquer avec les autres équipements du réseau. 1



Adresse IP	Adresse MAC

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 surveille le segment Ethernet pour mettre à jour sa table ARP avec les paires d'adresses IP-MAC afin de pouvoir envoyer les données à d'autres hôtes sur le LAN.

L'ordinateur 176.10.16.2 prépare les données à transmettre. Pour cela, il vérifie le câble réseau pour savoir s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, l'ordinateur 176.10.16.2 doit attendre, car les données ne peuvent être transmises que par un seul ordinateur à la fois. Le câble est disponible et l'ordinateur 176.10.16.2 peut effectuer la transmission.

L'ordinateur 176.10.16.2 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée. Une partie de ce processus consiste à ajouter les adresses source IP-MAC à la table ARP. La trame des données est ignorée par toutes les unités, à l'exception de celle à laquelle les données ont été envoyées.

L'ordinateur 176.10.16.3 prépare les données à transmettre. Il effectue toutes les étapes de la préparation.

L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

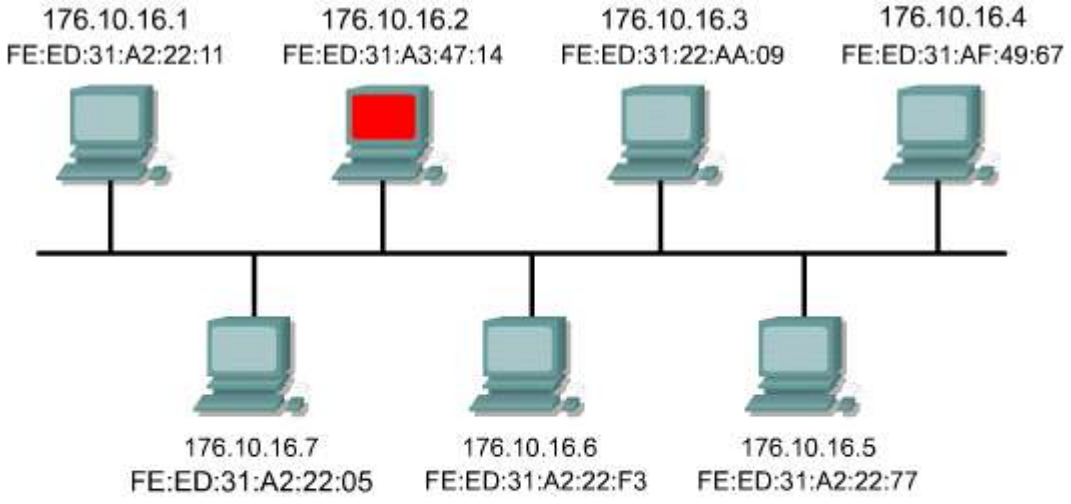
À nouveau, tous les hôtes du même segment analysent les trames entrantes. Ils ajoutent les données à leurs tables ARP et ignorent la trame si les données ne leurs sont pas destinées.

L'ordinateur 176.10.16.6 prépare les données à transmettre.

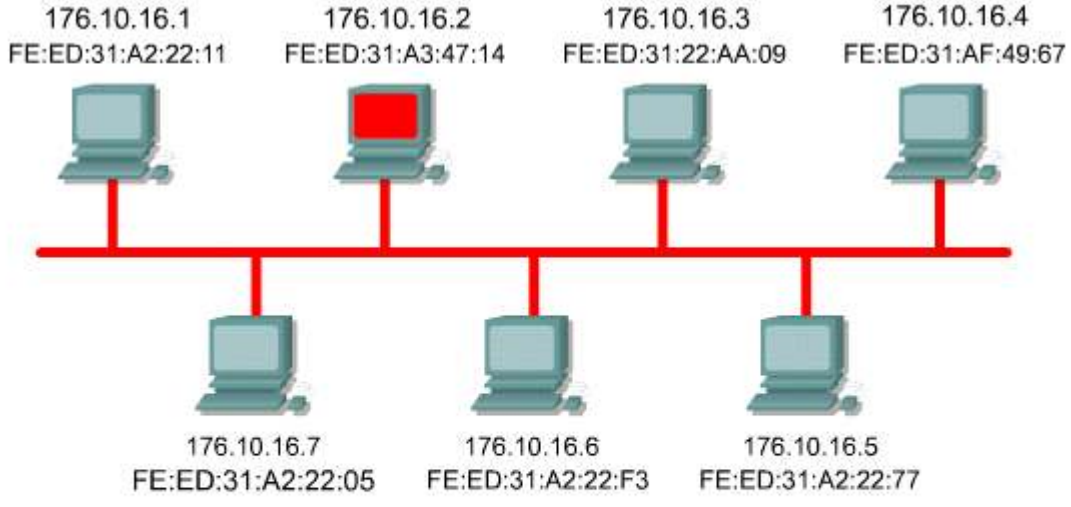
L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes. Ils ajoutent les données à leurs tables ARP et ignorent la trame si les données ne leurs sont pas destinées. Cela correspond au processus automatique utilisé sur un LAN Ethernet normal pour gérer les associations d'adresses.

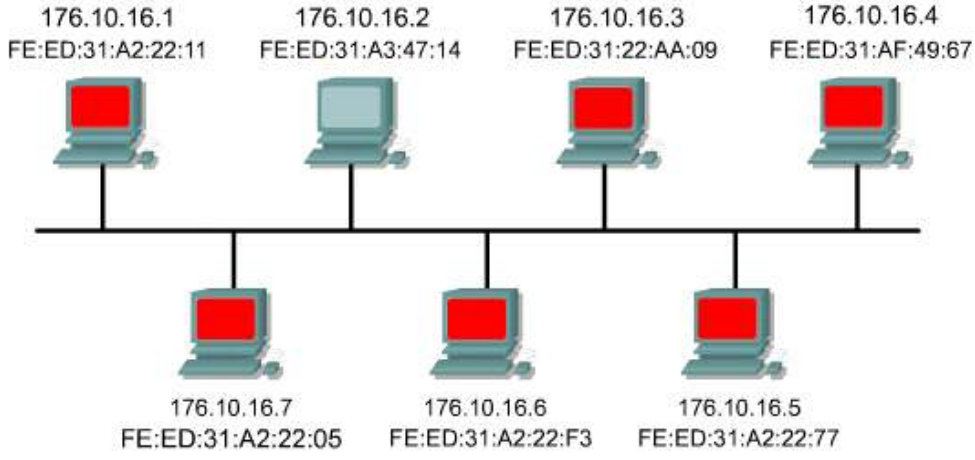
L'ordinateur 176.10.16.1 souhaite envoyer les données à l'ordinateur 176.10.16.4. Il dispose d'une adresse IP, mais la transmission des données nécessite aussi l'adresse MAC de l'ordinateur 176.10.16.4. Comment peut-il obtenir cette adresse MAC pour transmettre les données ?



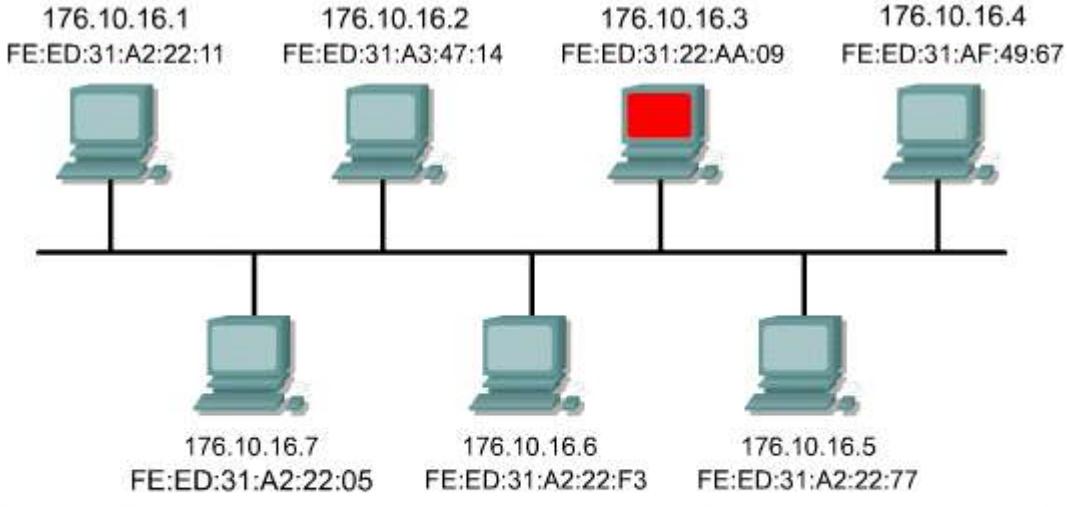
Adresse IP	Adresse MAC



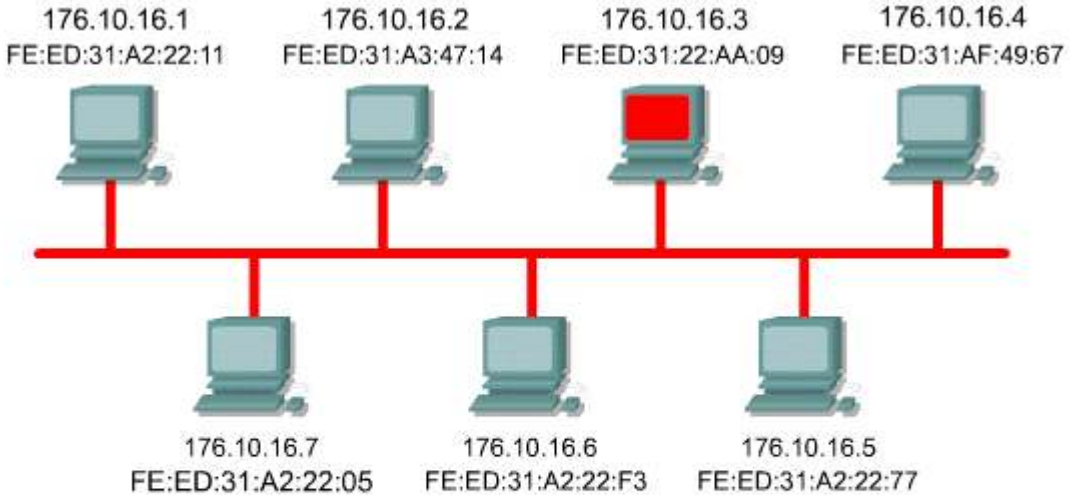
Adresse IP	Adresse MAC



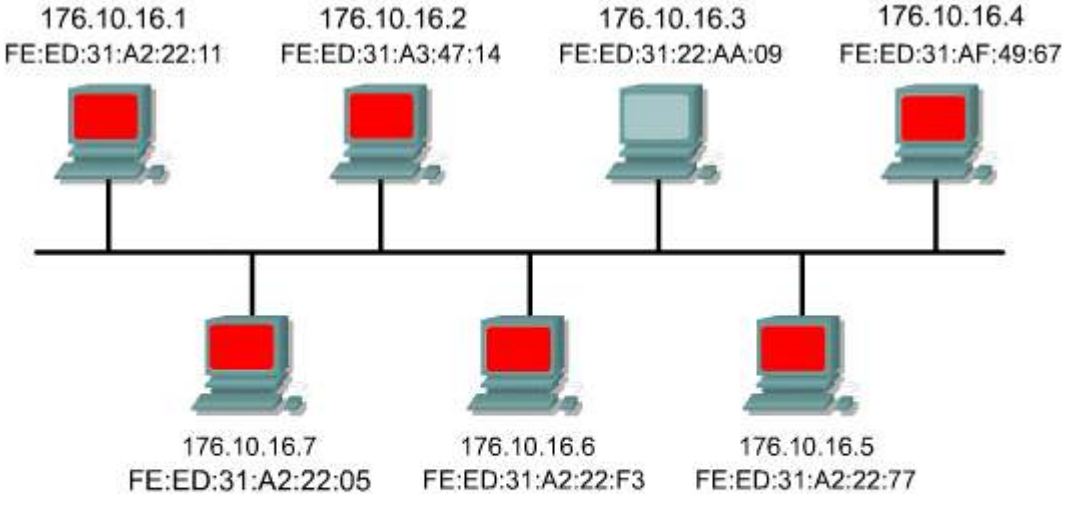
Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14



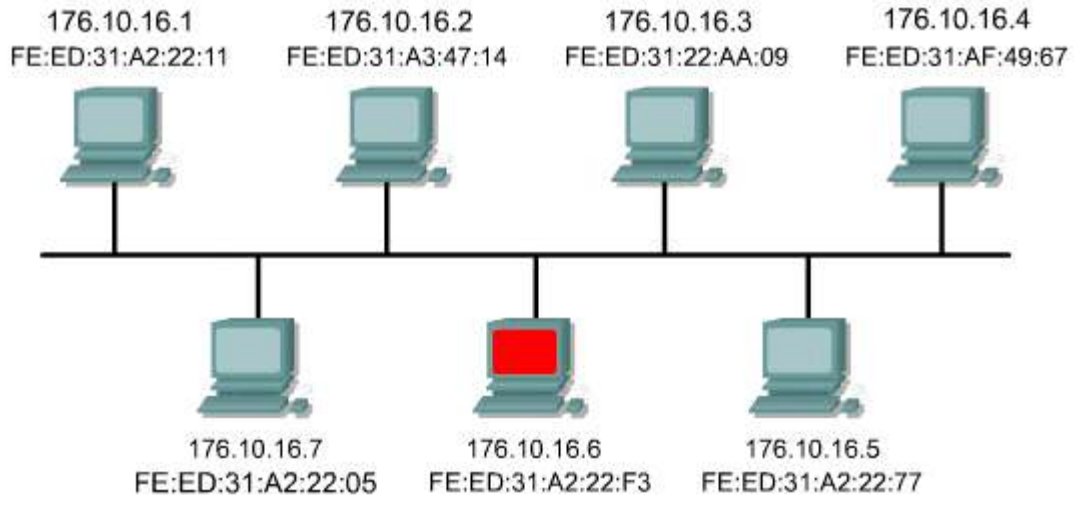
Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14



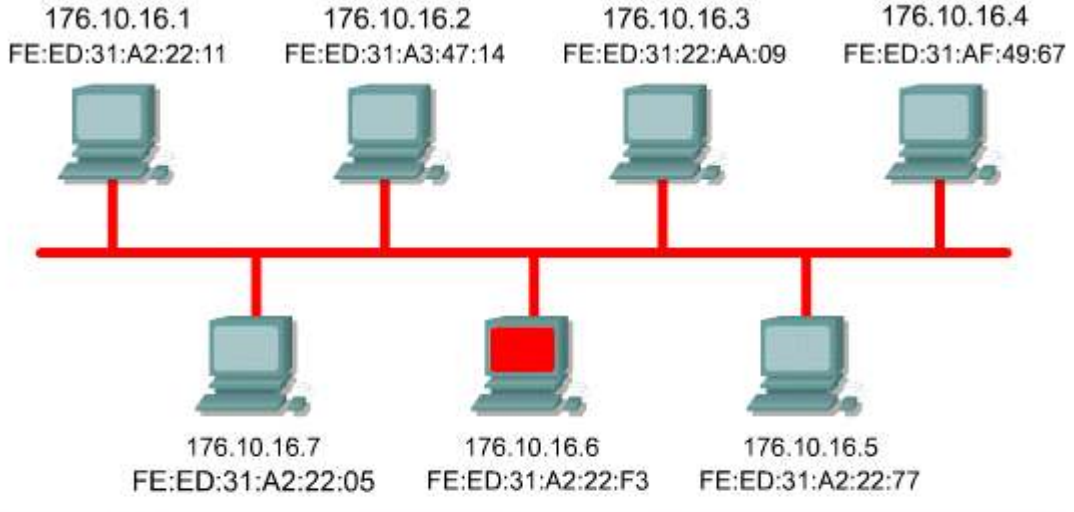
Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14



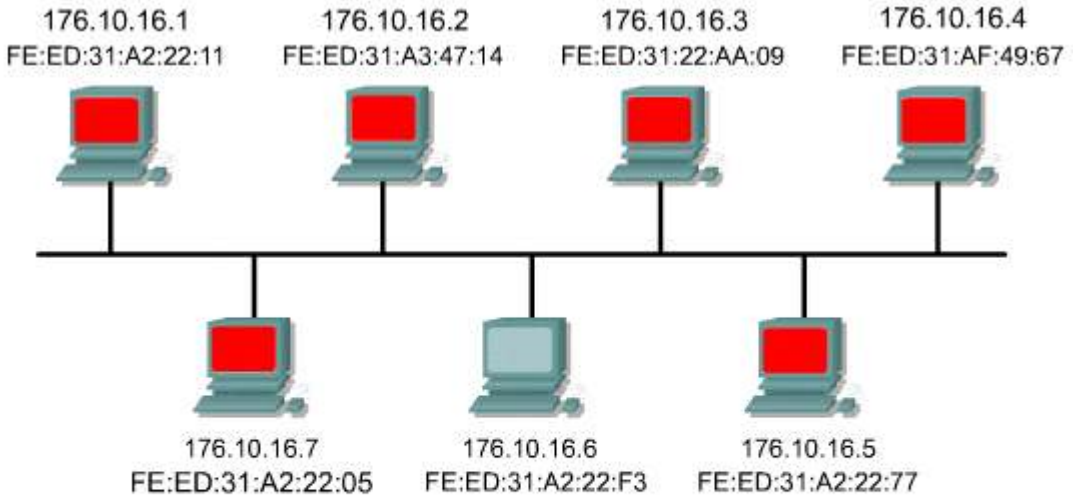
Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09



Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09

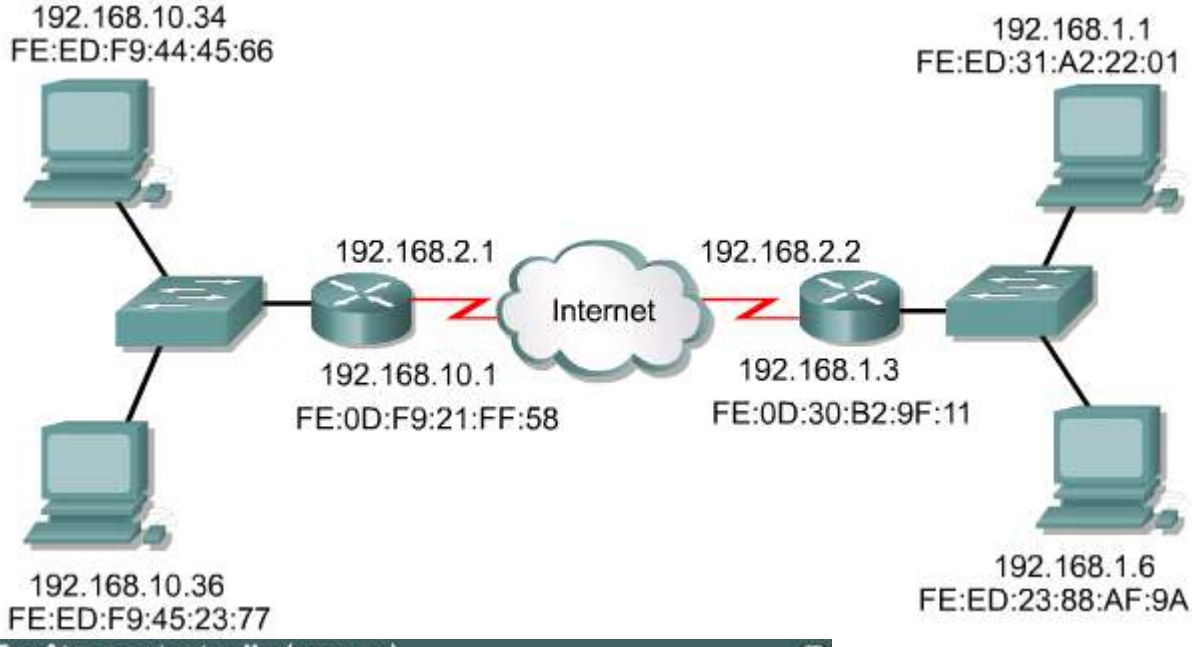


Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09



Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

Lors des échanges TCP/IP, un datagramme appartenant à un réseau local doit comporter une adresse MAC et une adresse IP de destination. Ces adresses doivent être valides et elles doivent correspondre aux adresses MAC et IP de destination de l'équipement hôte. Si elles ne correspondent pas, le datagramme est rejeté par l'hôte de destination. Pour échanger des données dans un segment LAN, deux adresses sont requises. Une solution de mappage automatique des adresses IP avec des adresses MAC est également requise. Le mappage manuel de ces adresses se révélerait beaucoup trop long. La pile de protocoles TCP/IP comprend un protocole appelé «ARP» (*Address Resolution Protocol*) qui peut obtenir automatiquement les adresses MAC pour la transmission locale. Plusieurs problèmes apparaissent lors de l'envoi des données à l'extérieur du réseau local.



Fenêtre contextuelle (pop up)

L'ordinateur 192.168.10.34 doit communiquer avec l'ordinateur 192.168.1.1. Comment obtient-il l'adresse MAC de l'ordinateur 192.168.1.1, et l'obtention de cette adresse présente-t-elle des avantages ? Les adresses MAC sont utiles uniquement dans un réseau local. Elles sont donc inutiles en dehors du réseau 192.168.10.0. Ainsi, l'adresse MAC du routeur est nécessaire pour extraire les données du LAN et les transférer au système WAN.

Pour échanger des données entre deux segments LAN, un élément supplémentaire est requis. Les adresses IP et MAC sont nécessaires à l'hôte de destination et à l'équipement de routage intermédiaire. Proxy ARP est une variante du protocole ARP qui fournit l'adresse MAC d'un équipement intermédiaire pour la transmission de données vers un autre segment du réseau en dehors du LAN.

La page suivante présente le protocole ARP (*Address Resolution Protocol*).

9.3 Obtention d'une adresse IP

9.3.7 Protocole ARP (Address Resolution Protocol)

Cette page explique le mécanisme du protocole ARP.

Dans un réseau TCP/IP, un paquet de données doit contenir une adresse MAC de destination et une adresse IP de destination. Si l'une ou l'autre est manquante, les données qui se trouvent au niveau de la couche 3 ne sont pas transmises aux couches supérieures. Ainsi, les adresses MAC et IP se contrôlent et s'équilibrent mutuellement. Une fois que les équipements ont déterminé les adresses IP des équipements de destination, ils peuvent ajouter les adresses MAC de destination aux paquets de données.

Certains tiennent à jour des tables contenant les adresses MAC et IP des autres équipements connectés au même réseau local. 1

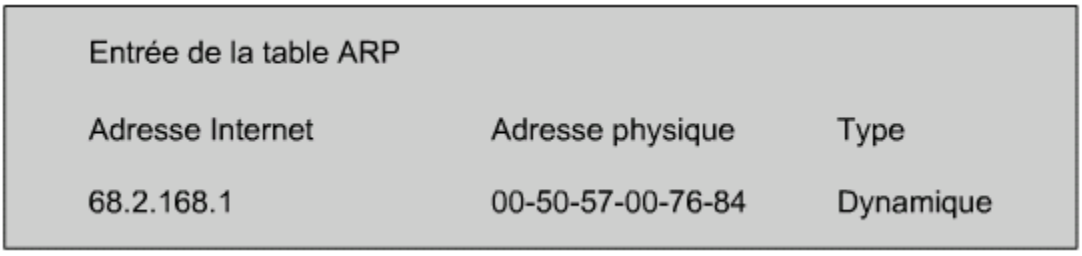


Table ARP 198.150.11.36

MAC	IP
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:00:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35

Ces tables sont appelées «tables ARP». Elles sont stockées dans la mémoire RAM, où les informations en mémoire cache sont mises à jour automatiquement dans chaque équipement. Il est très rare qu'un utilisateur ait à entrer manuellement des informations dans une table ARP. Tout équipement du réseau met à jour sa propre table ARP. Si un équipement cherche à envoyer des données sur le réseau, il utilise les informations contenues dans la table ARP.

Lorsqu'une source détermine l'adresse IP d'une destination, elle consulte la table ARP pour trouver l'adresse MAC de destination. Une fois l'entrée recherchée trouvée dans sa table (adresse IP de destination correspondant à l'adresse MAC de destination), elle associe l'adresse IP à l'adresse MAC et l'utilise pour encapsuler les données. Le paquet de données est alors envoyé à l'équipement de destination via le média réseau.

Les équipements disposent de deux méthodes pour obtenir les adresses MAC à ajouter aux données encapsulées. L'une d'elles consiste à surveiller le trafic existant sur le segment du réseau local. 2

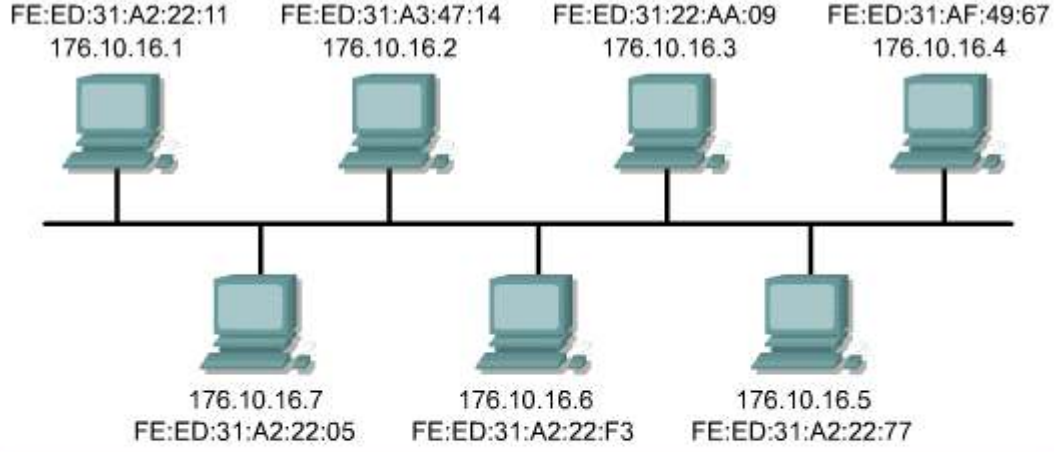


Table ARP

Adresse IP	Adresse MAC

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 surveille le segment Ethernet pour mettre à jour sa table ARP.

L'ordinateur 176.10.16.2 prépare les données à transmettre. Pour cela, il vérifie le câble réseau pour savoir s'il est utilisé par un autre ordinateur. Si une autre station utilise le câble, l'ordinateur 176.10.16.2 doit attendre, car les données ne peuvent être transmises que par un seul ordinateur à la fois. Le câble est disponible et l'ordinateur 176.10.16.2 peut effectuer la transmission.

L'ordinateur 176.10.16.2 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée. Une partie de ce processus consiste à ajouter les adresses source IP-

MAC des données à la table ARP.

L'ordinateur 176.10.16.3 prépare les données à transmettre. Il effectue toutes les étapes de la préparation.

L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du segment analysent les trames entrantes et ajoutent les données à leurs tables ARP.

L'ordinateur 176.10.16.6 prépare les données à transmettre.

L'ordinateur 176.10.16.6 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes.

L'ordinateur 176.10.16.5 prépare les données à transmettre. Le délai d'attente de la première paire de la table ARP a été atteint. Si un ordinateur ne transmet pas de données pendant un certain temps, sa paire IP-MAC est supprimée de la table ARP.

L'ordinateur 176.10.16.3 transmet ses trames de données via le segment Ethernet. La première valeur de la table ARP est supérieure à celle du délai d'attente. Elle est donc supprimée. La table ARP est mise à jour de façon dynamique. Les entrées sont ajoutées et supprimées selon l'activité du segment et les délais d'attente.

À nouveau, tous les hôtes du même segment analysent les trames entrantes. De nouvelles valeurs sont ajoutées à la table ARP.

L'ordinateur 176.10.16.2 prépare les données à transmettre.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée. La paire IP-MAC de l'ordinateur 176.10.16.2 est à nouveau ajoutée à la table. Si cette transmission avait été effectuée avant le dépassement du délai d'attente, la paire n'aurait pas été supprimée de la table, et le délai d'attente aurait simplement été réinitialisé.

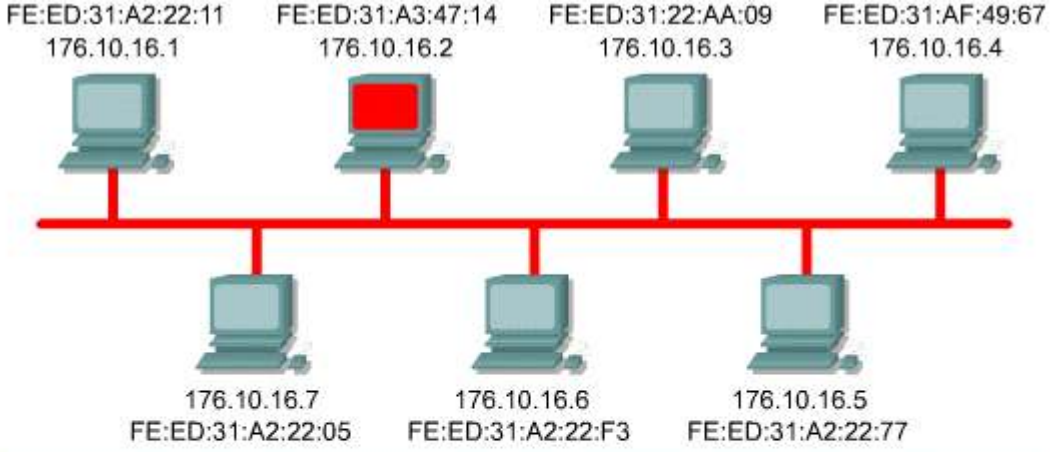


Table ARP

Adresse IP	Adresse MAC

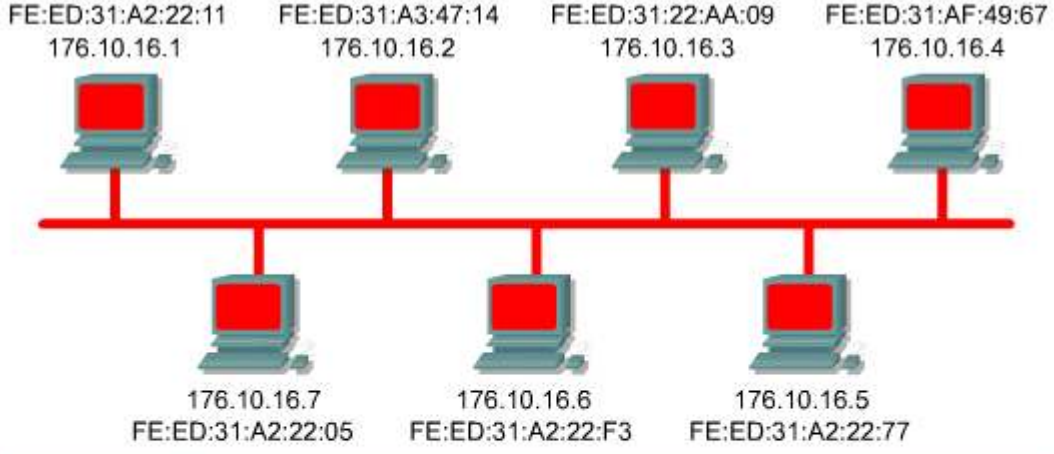


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14

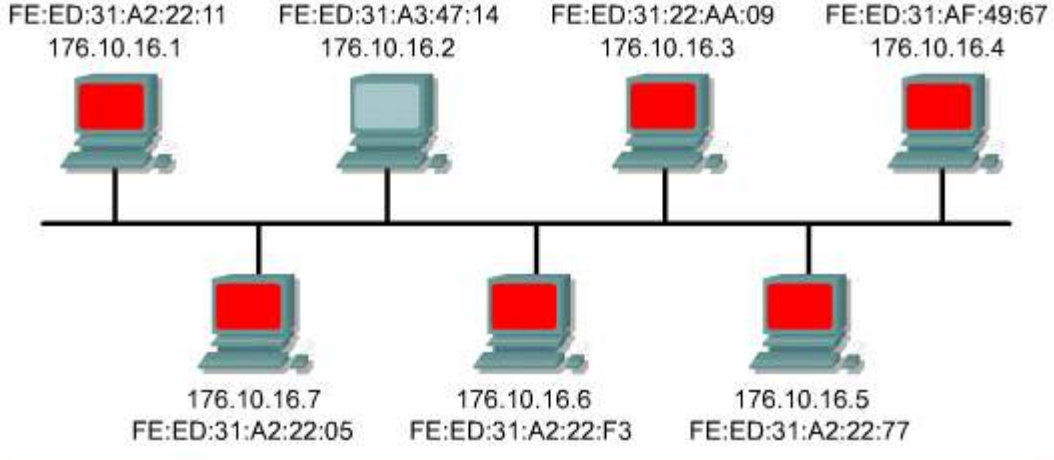


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14

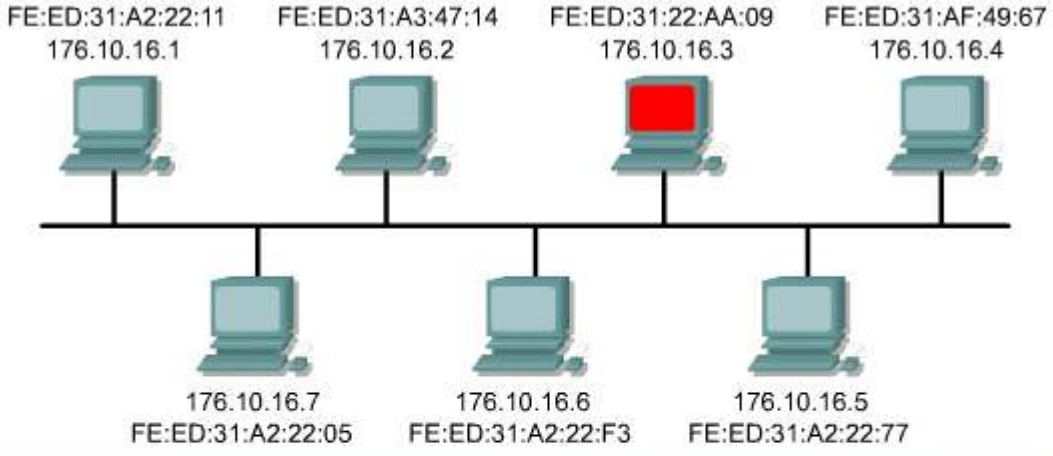


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14

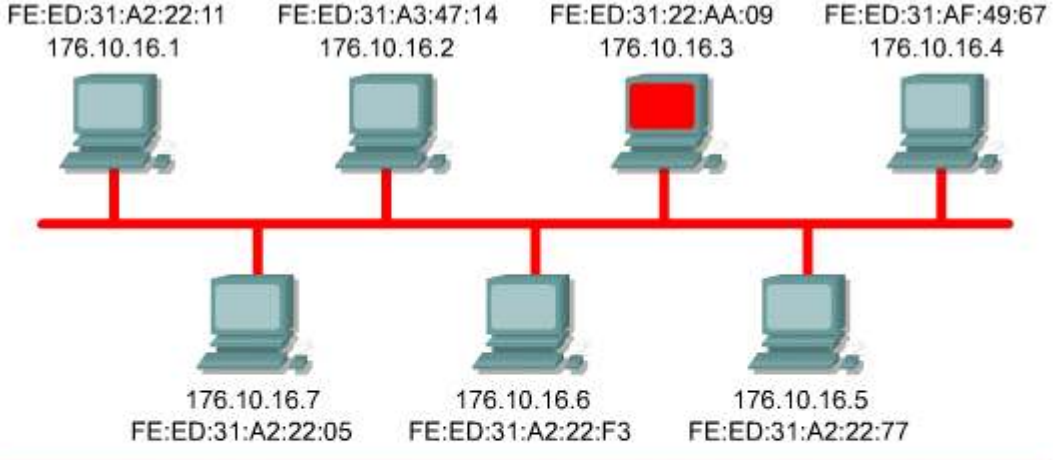


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14

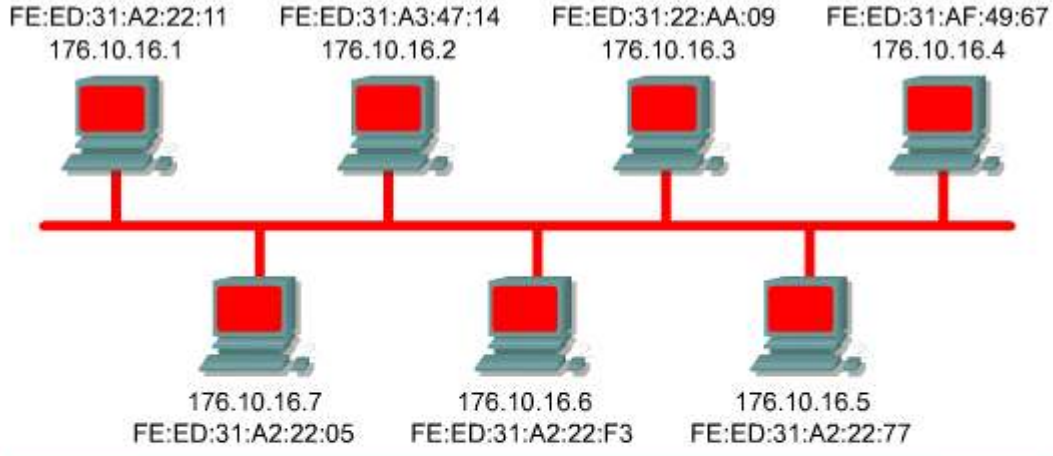


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09

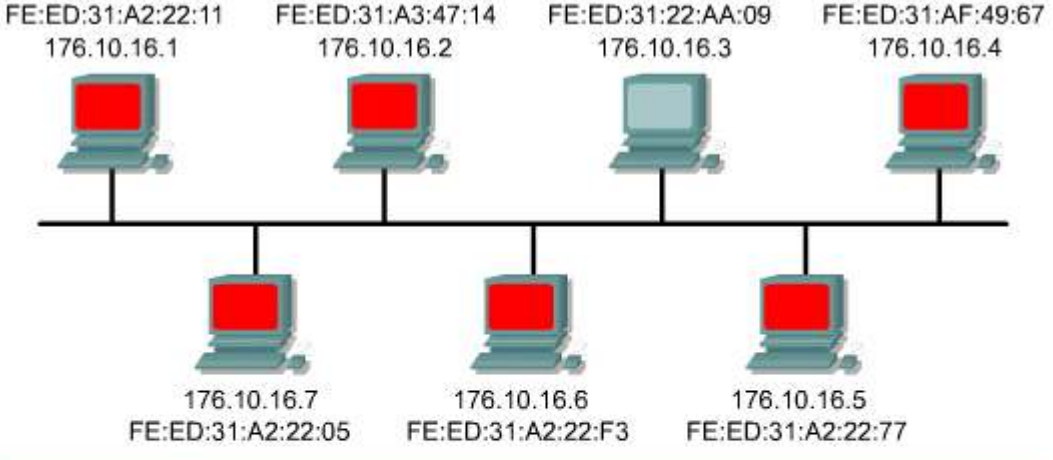


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09

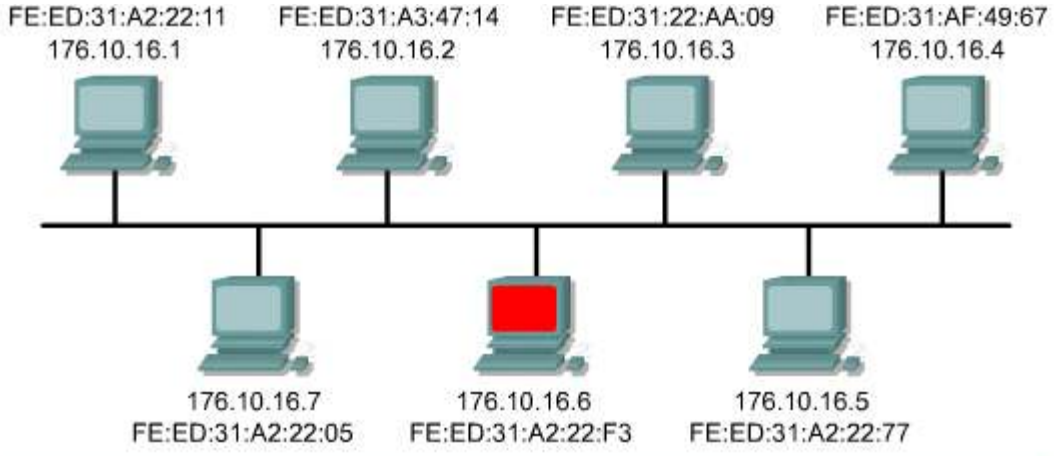


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09

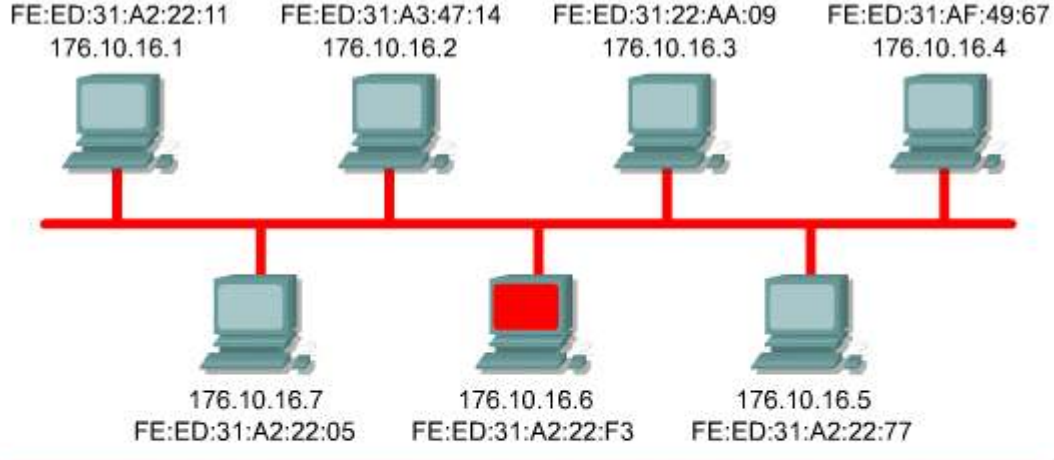


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09

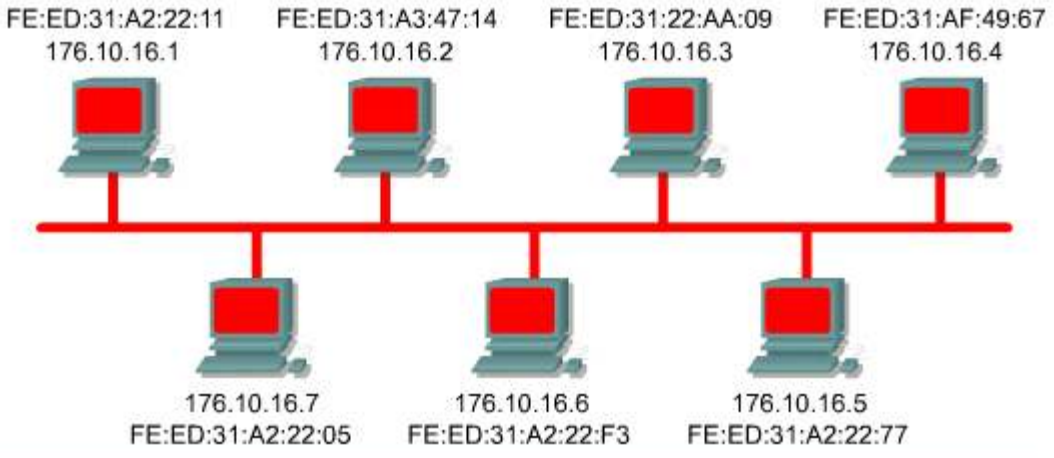


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

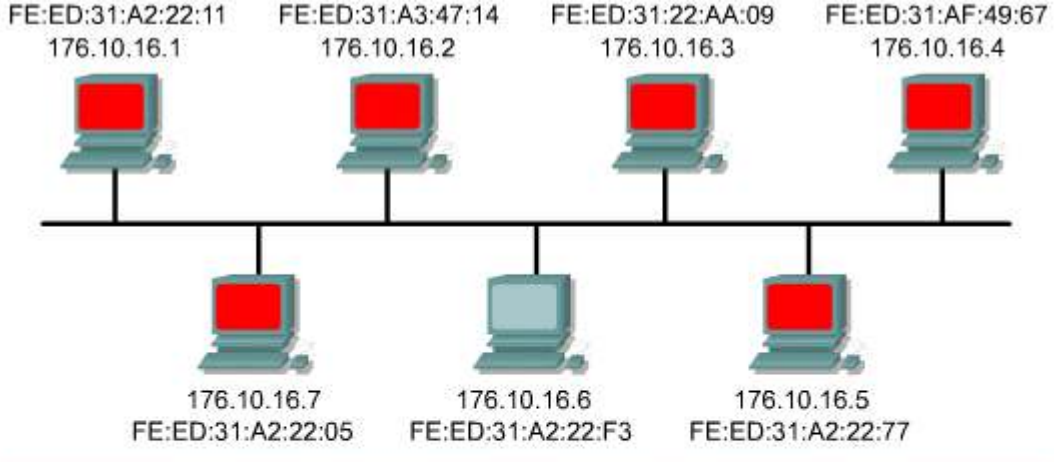


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

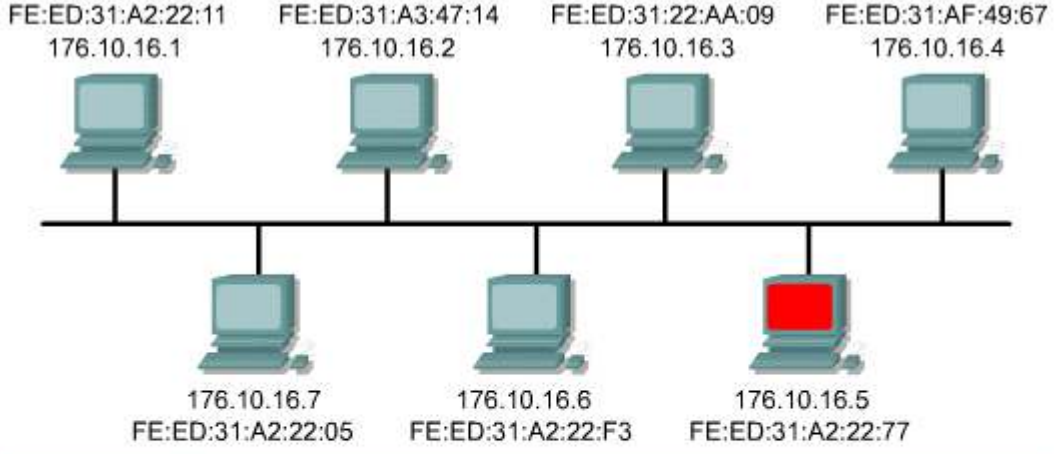


Table ARP

Adresse IP	Adresse MAC
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

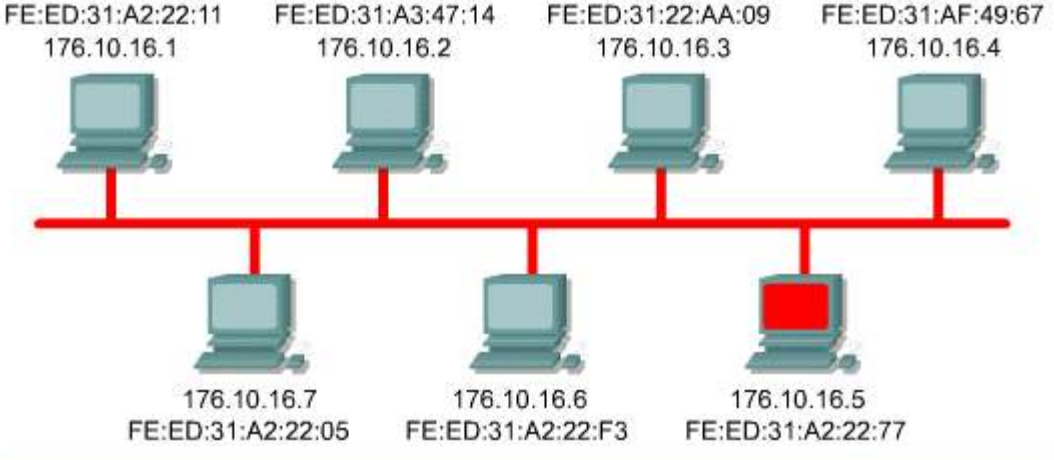


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3

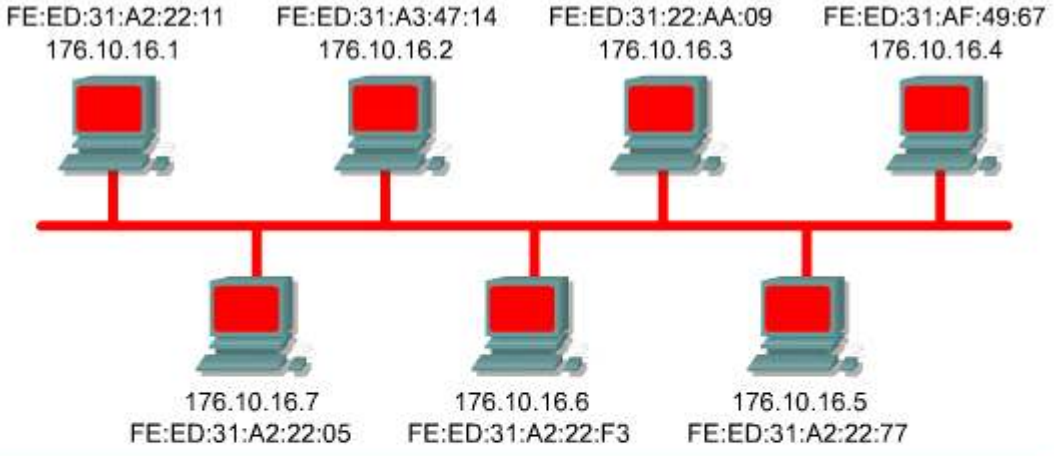


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77

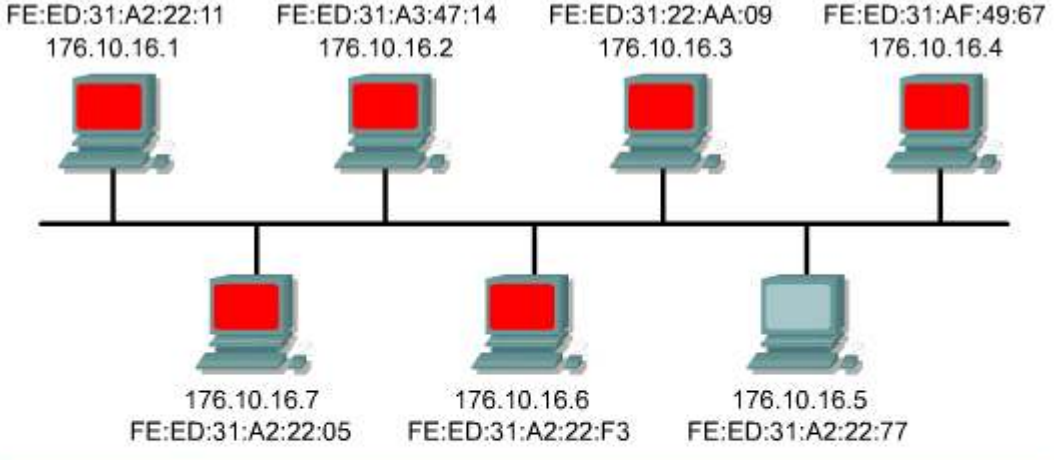


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77

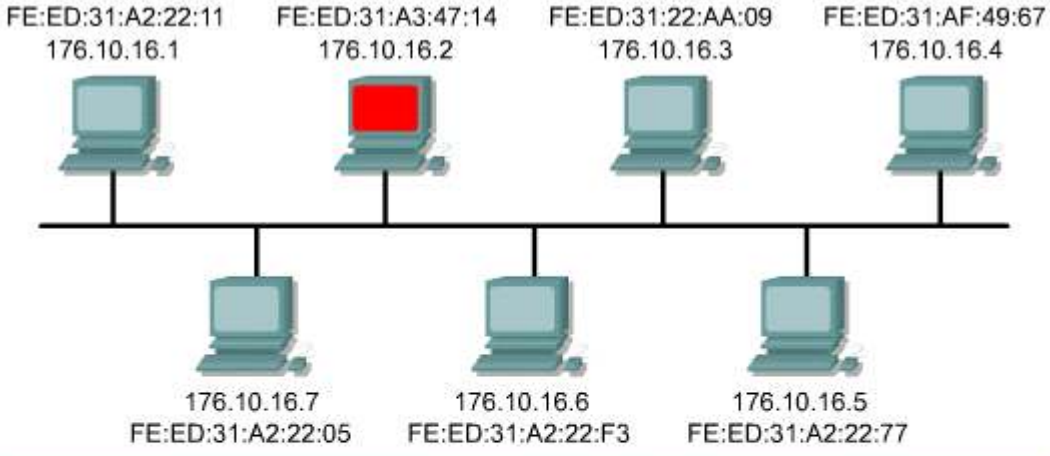


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77

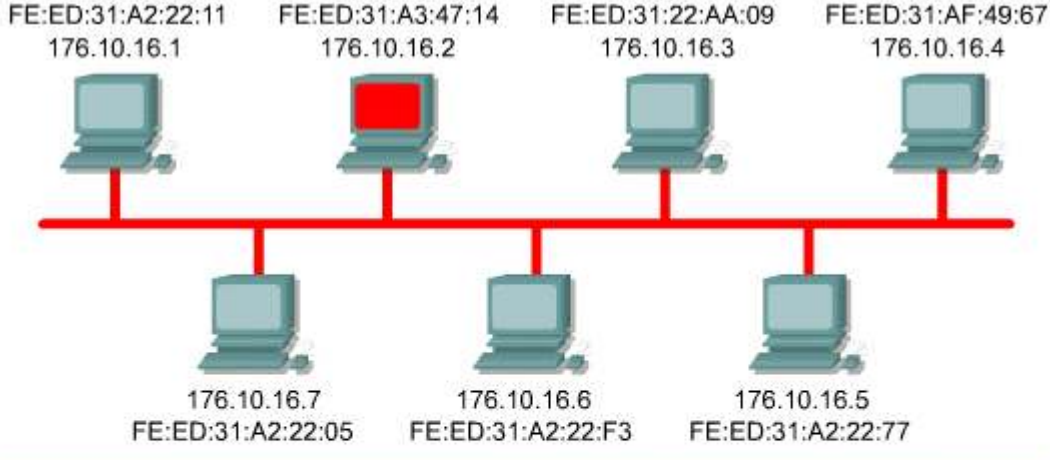


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77

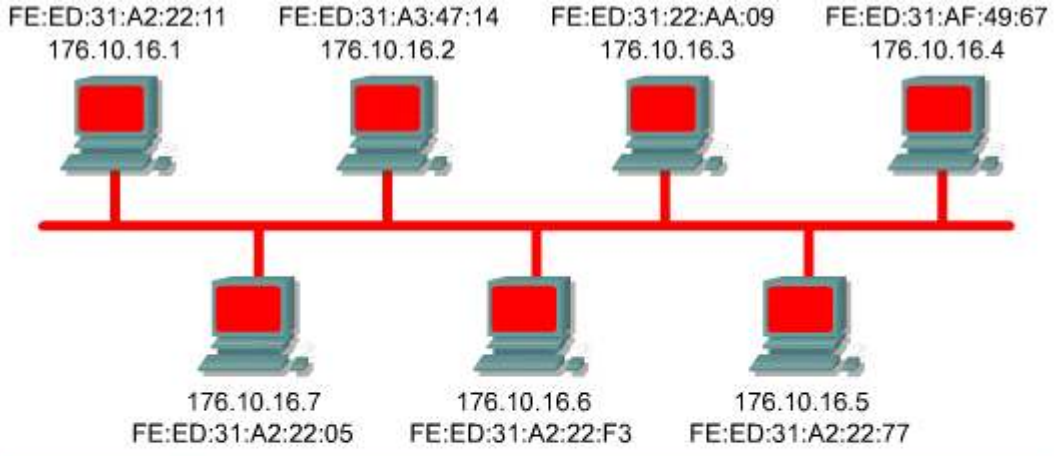


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

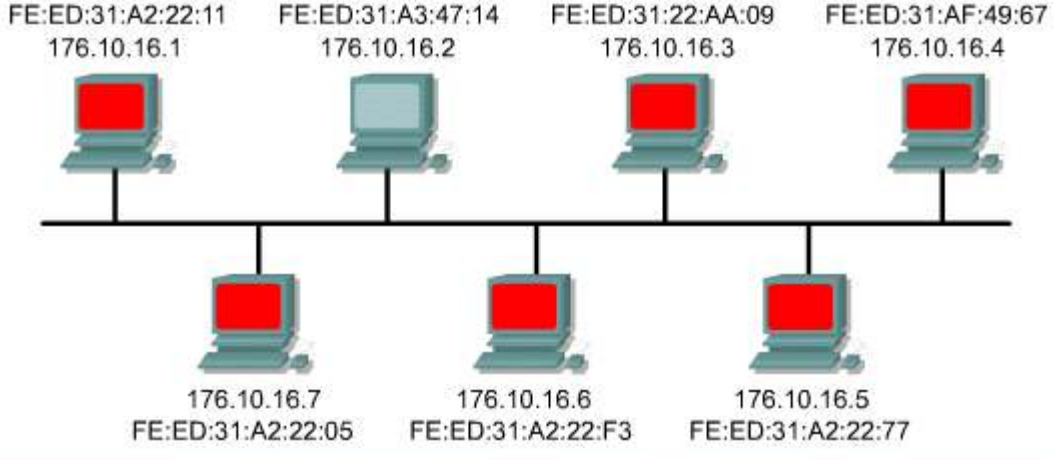
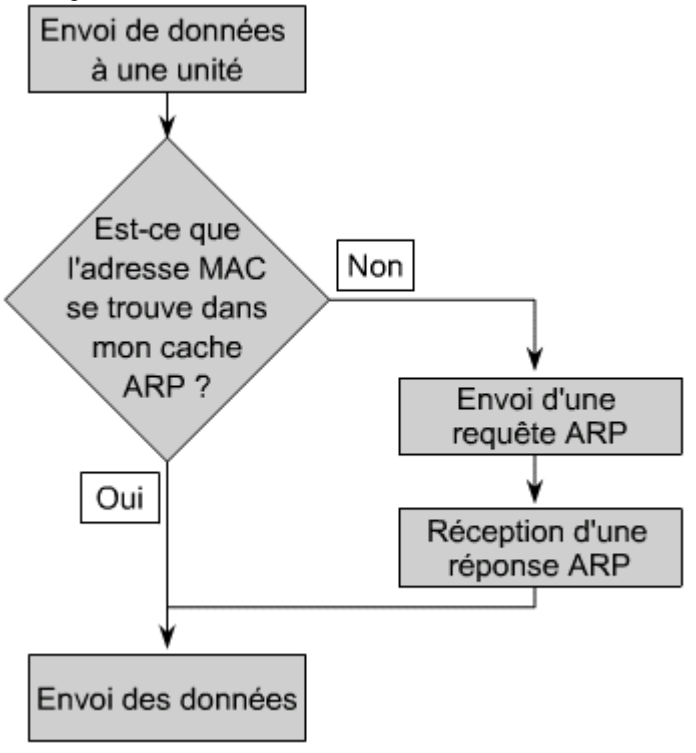


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Toutes les stations du réseau Ethernet analysent le trafic afin de déterminer si la transmission leur est destinée. Une partie de ce processus consiste à enregistrer les adresses source IP et MAC du datagramme dans une table ARP. Ainsi, les paires d'adresses sont intégrées à la table ARP lors de l'envoi des données sur le réseau. L'autre solution qui permet d'obtenir une paire d'adresses pour la transmission des données consiste à diffuser

une requête ARP. 3 4


Envoi de données à une unité
Est-ce que l'adresse MAC se trouve dans mon cache ARP ?
Non
Oui
Envoi d'une requête ARP
Réception d'une réponse ARP
Envoi des données

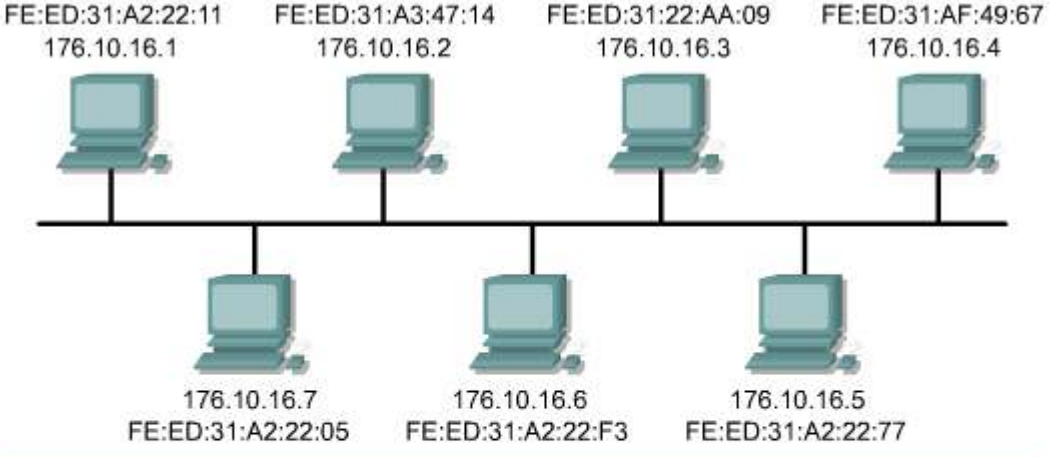


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 doit transmettre des données à l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 prépare les données à transmettre à l'ordinateur 176.10.16.4. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de l'ordinateur 176.10.16.4 ne se trouve pas dans sa table ARP. L'ordinateur 176.10.16.1 ayant besoin de cette paire, il doit émettre une requête ARP pour l'obtenir.

L'ordinateur 176.10.16.1 n'effectue pas le processus d'encapsulation pour la transmission des données mais crée une requête ARP pour obtenir l'adresse MAC de l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des données entrantes pour déterminer si la transmission leur est destinée.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse IP de destination des trames entrantes.

L'ordinateur 176.10.16.4 prépare les données de réponse ARP à transmettre.

L'ordinateur 176.10.16.4 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du segment analysent les trames entrantes et ajoutent les données à leurs tables ARP.

L'ordinateur 176.10.16.1 prépare les données à transmettre.

L'ordinateur 176.10.16.1 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

L'ordinateur 176.10.16.4 traite la transmission des données.

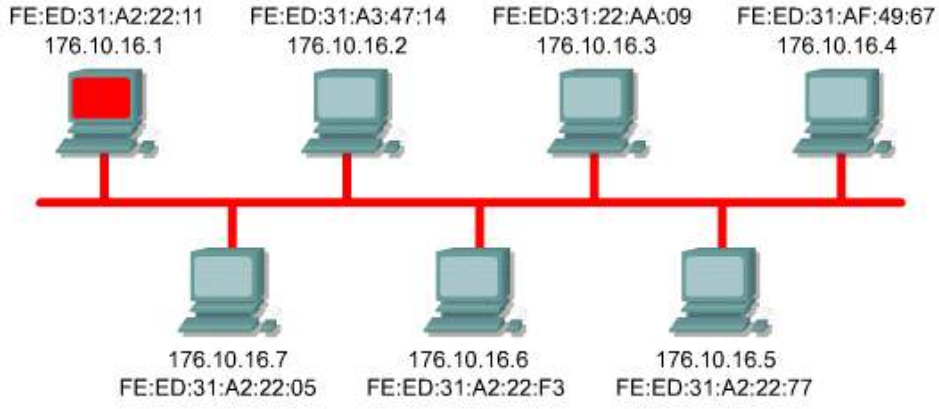


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

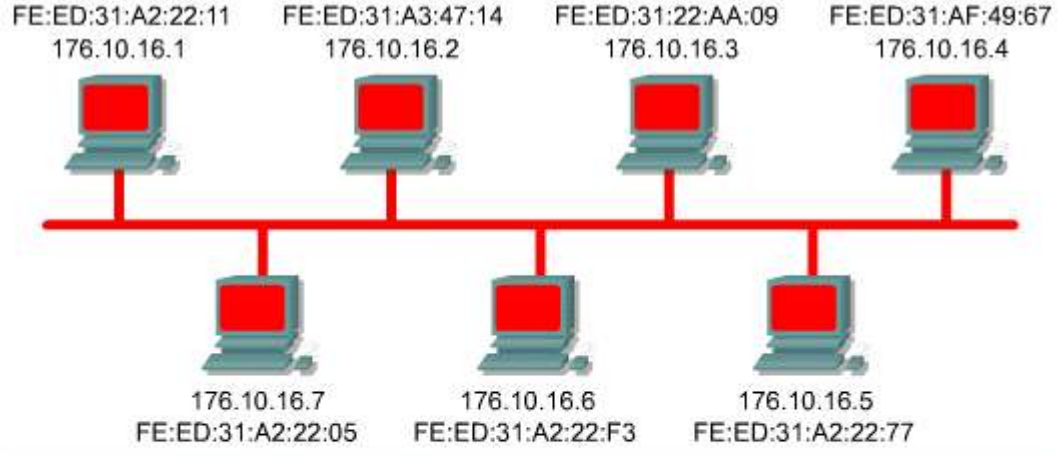


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

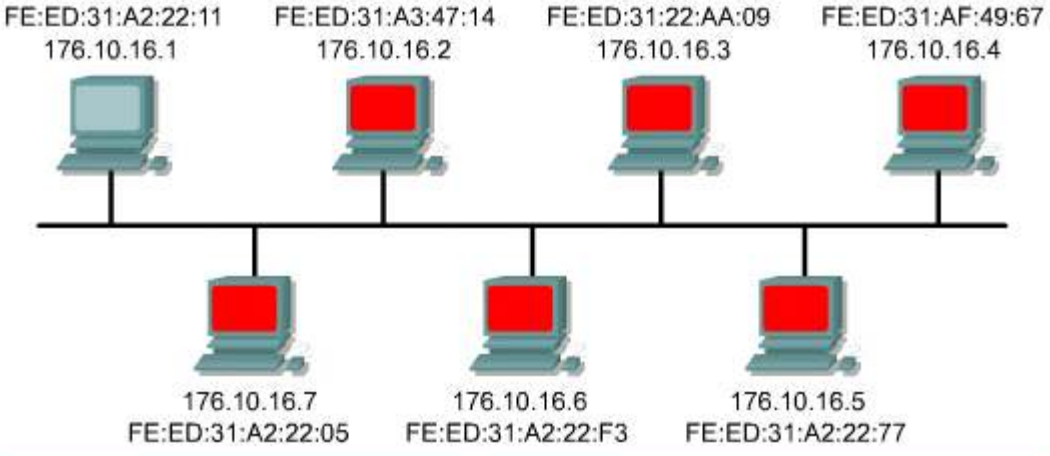


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

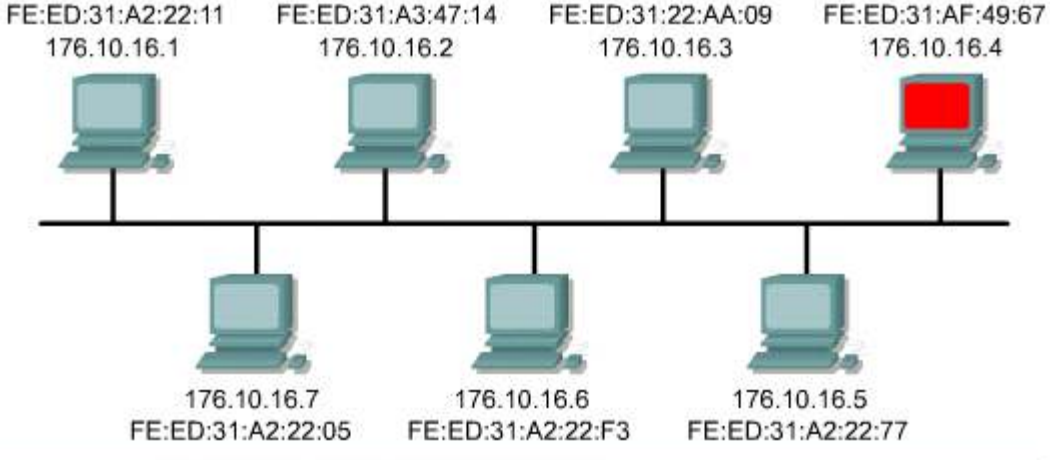


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

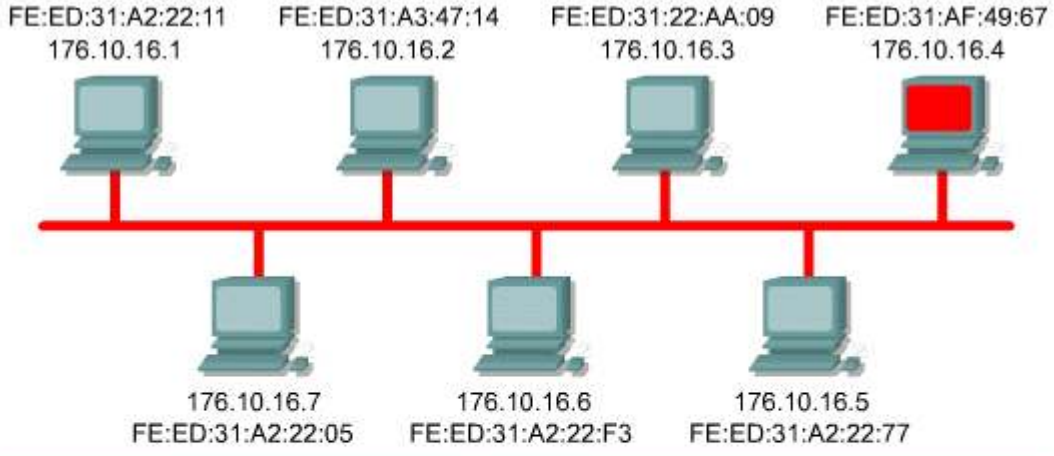


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

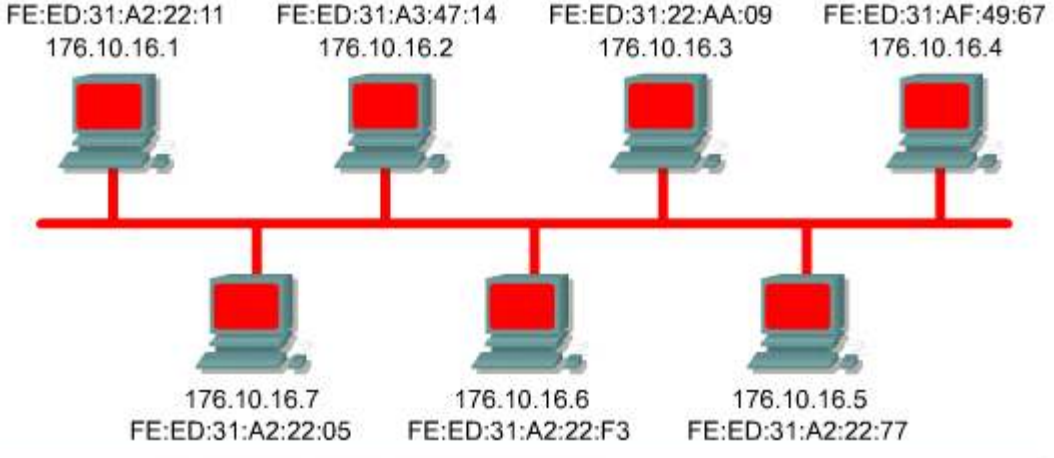


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

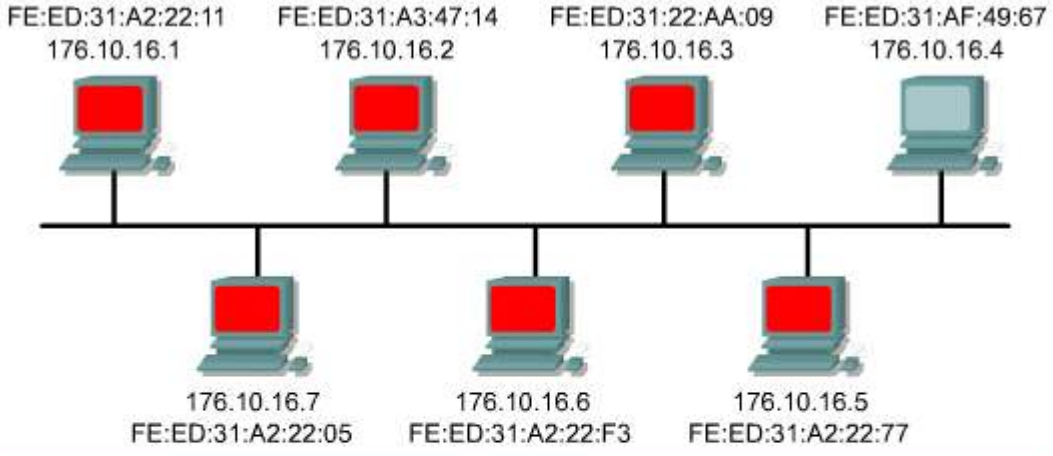


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

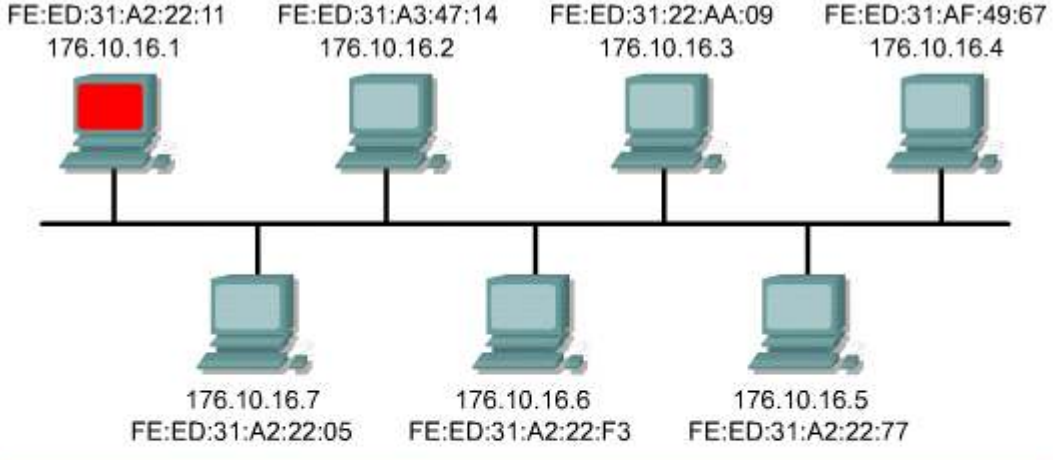


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

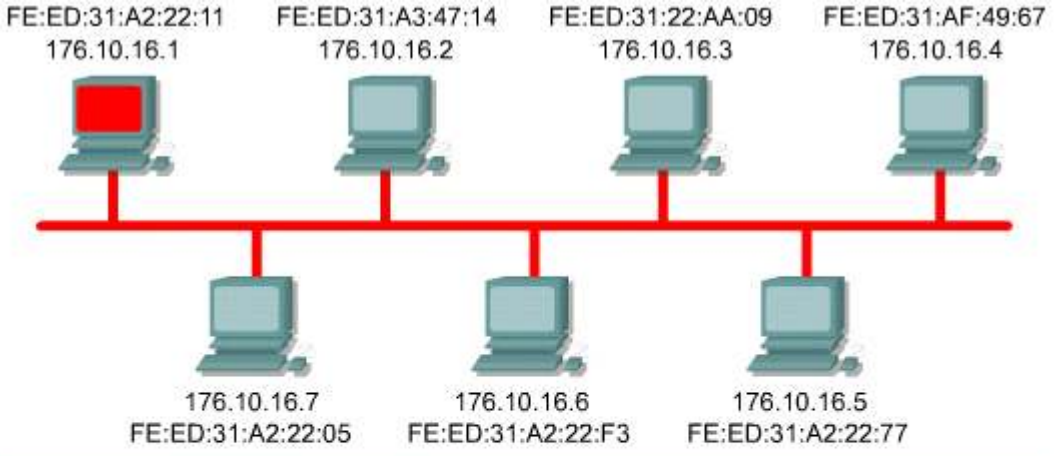


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

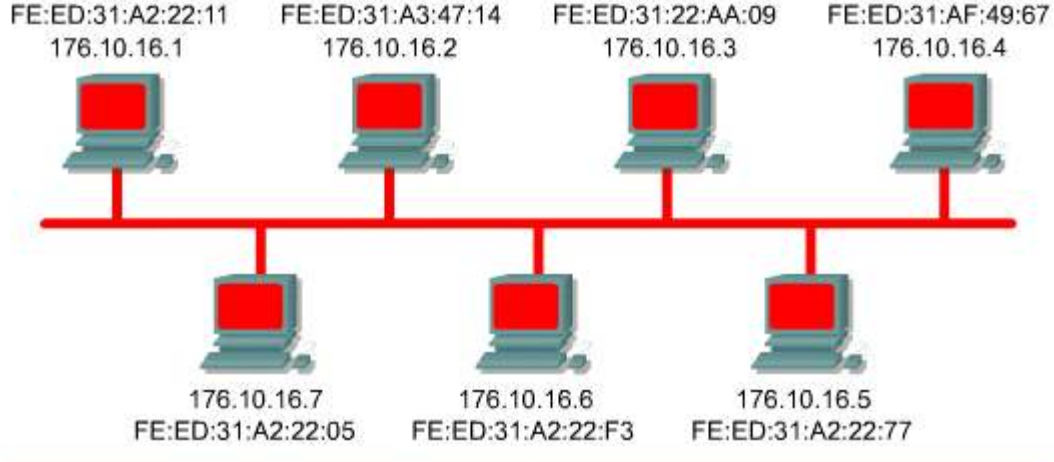


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

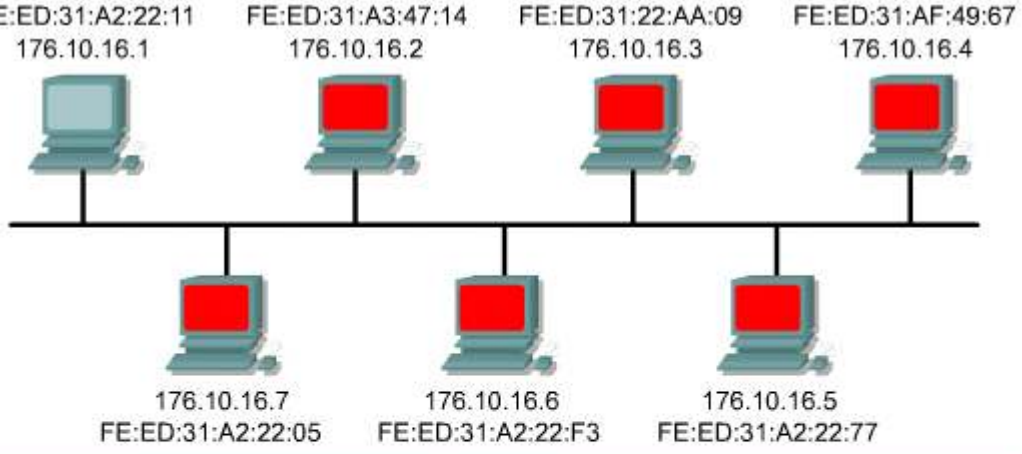


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

L'ordinateur qui a besoin d'une paire d'adresses IP et MAC diffuse une requête ARP. Tous les autres équipements du réseau local analysent ensuite cette requête. Si l'un des équipements correspond à l'adresse IP de la requête, il renvoie une réponse ARP avec sa paire d'adresses IP/MAC. Si l'adresse IP appartient au réseau local, mais que l'ordinateur est introuvable ou hors tension, aucune réponse n'est faite à la requête ARP. Dans ce cas, l'équipement source génère une erreur. Si la requête appartient à un réseau IP différent, un autre processus doit être utilisé.

Les routeurs ne transmettent pas les paquets de broadcast. Lorsque la fonction est activée, le routeur exécute une requête via Proxy ARP. 5

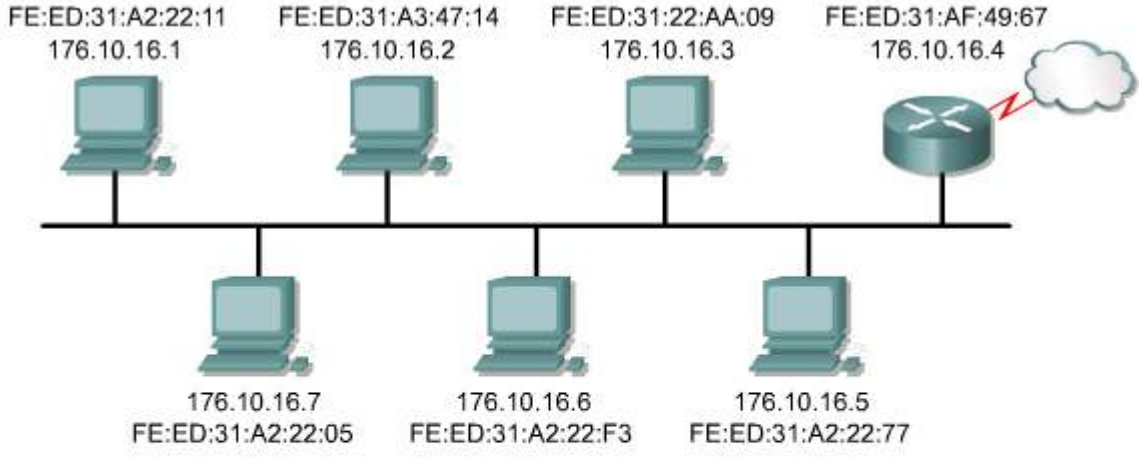


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 doit transmettre des données à routeur 176.10.16.4.

L'ordinateur 176.10.16.1 prépare les données à transmettre à routeur 176.10.16.4. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de routeur 176.10.16.4 ne se trouve pas dans sa table ARP. L'ordinateur 176.10.16.1 ayant besoin de cette paire, il doit émettre une requête ARP pour l'obtenir.

L'ordinateur 176.10.16.1 n'effectue pas le processus d'encapsulation pour la transmission des données mais crée une requête ARP pour obtenir l'adresse MAC de l'ordinateur 176.10.16.4.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les ordinateurs du segment Ethernet analysent les trames des

données entrantes pour déterminer si la transmission leur est destinée.

Toutes les unités, à l'exception du routeur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse IP de destination des trames entrantes.

Le routeur 176.10.16.4 compare l'adresse avec son adresse IP de l'interface Ethernet. Grâce à cette opération, il constate que ce paquet est acheminé en dehors du LAN. Ce routeur étant compatible avec le protocole Proxy ARP, il prépare une réponse ARP à l'hôte demandeur avec son adresse MAC et l'adresse IP de l'unité de destination.

Le routeur 176.10.16.4 transmet ses trames de données via le segment Ethernet.

À nouveau, tous les hôtes du segment analysent les trames entrantes et ajoutent les données à leurs tables ARP.

L'ordinateur 176.10.16.1 prépare les données à transmettre.

L'ordinateur 176.10.16.1 transmet ses trames de données via le segment Ethernet.

Tous les hôtes du même segment analysent les trames entrantes.

Tous les ordinateurs, à l'exception de l'ordinateur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

Le routeur 176.10.16.4 prend en charge la transmission des données vers le prochain saut du réseau.

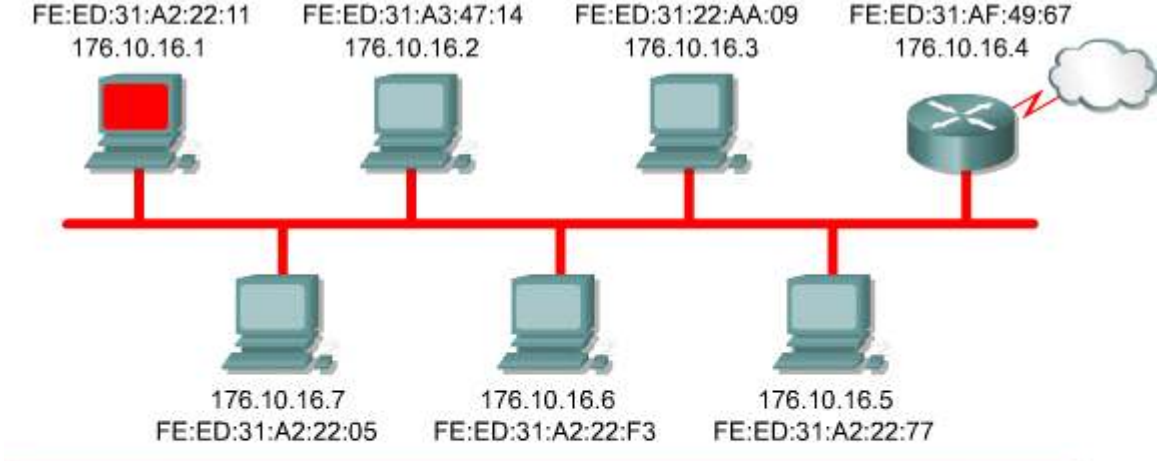


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

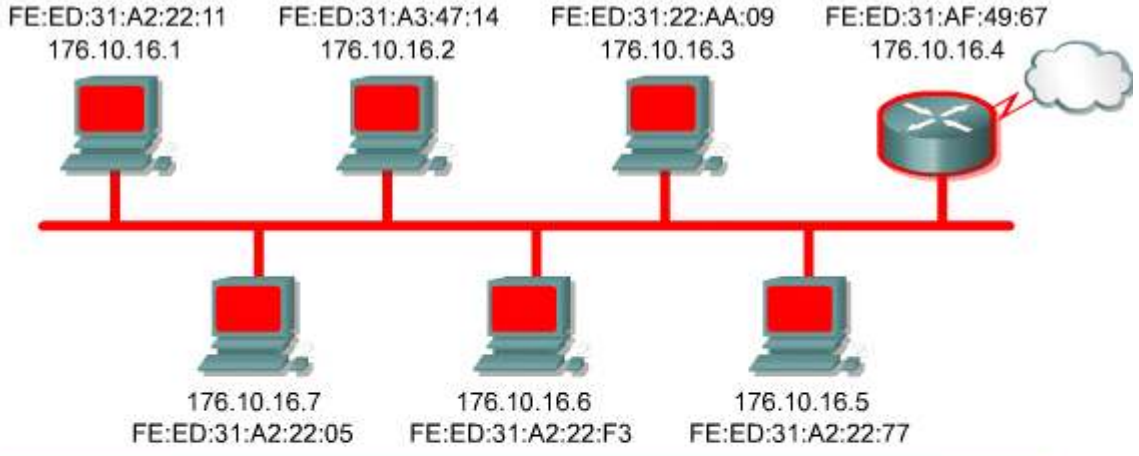


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

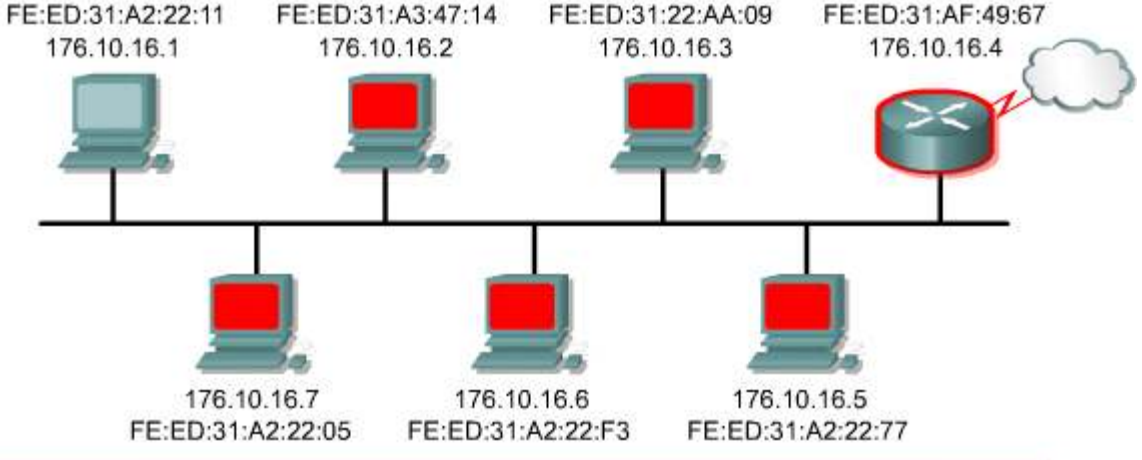


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

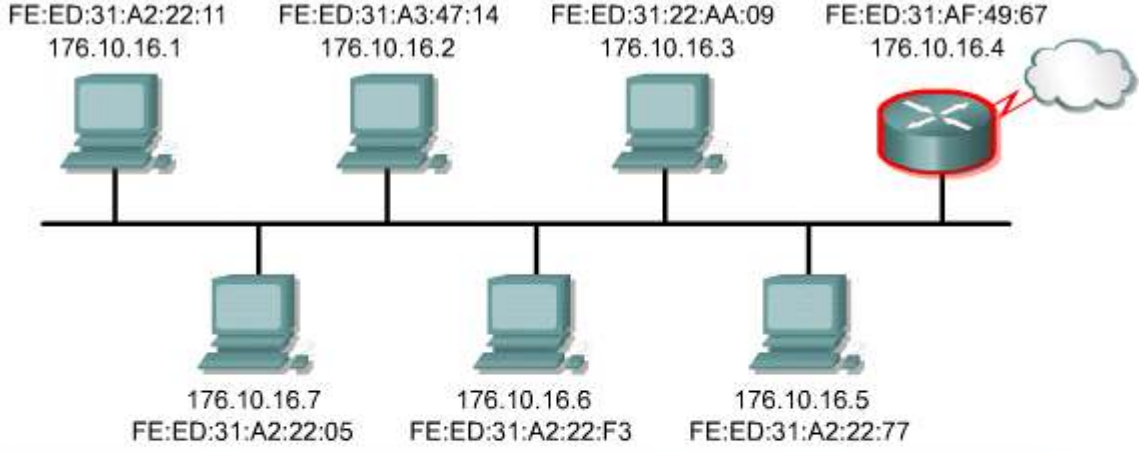


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

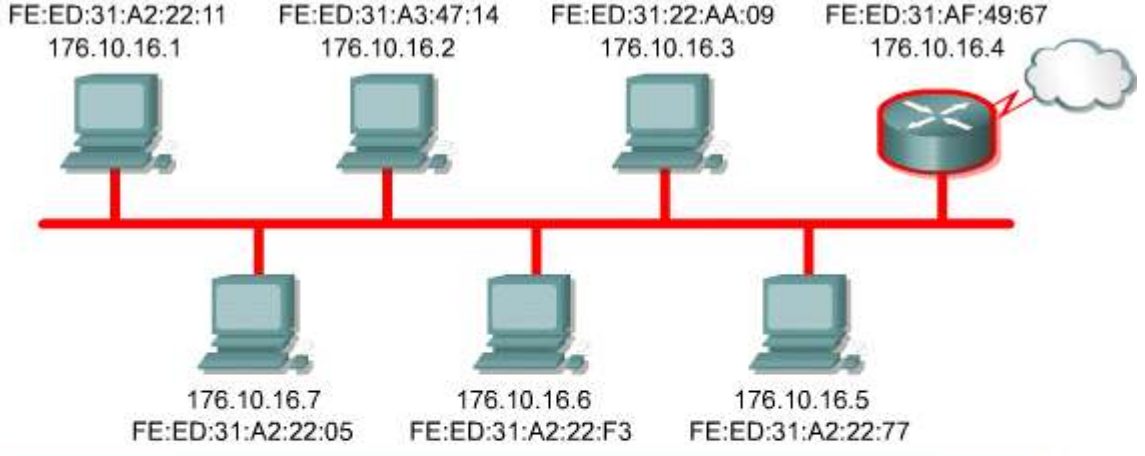


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

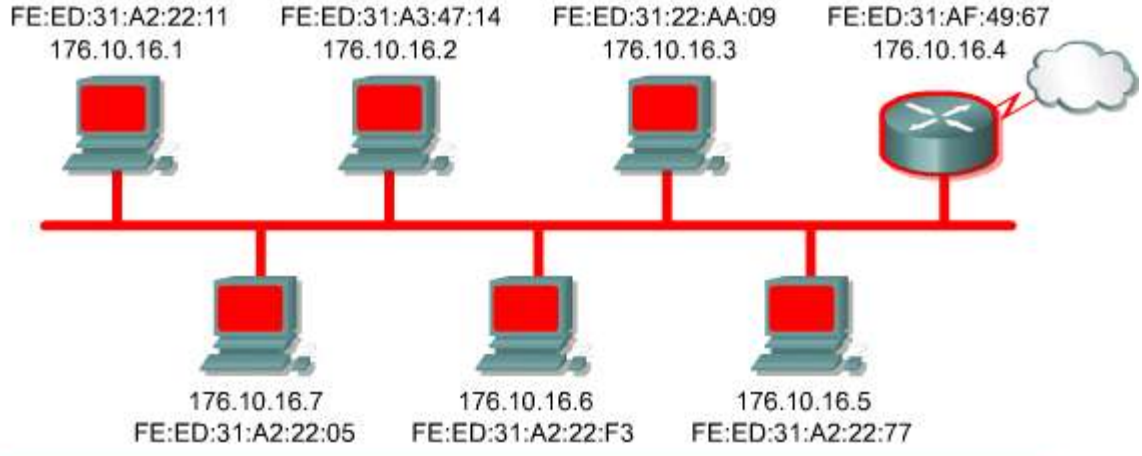


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

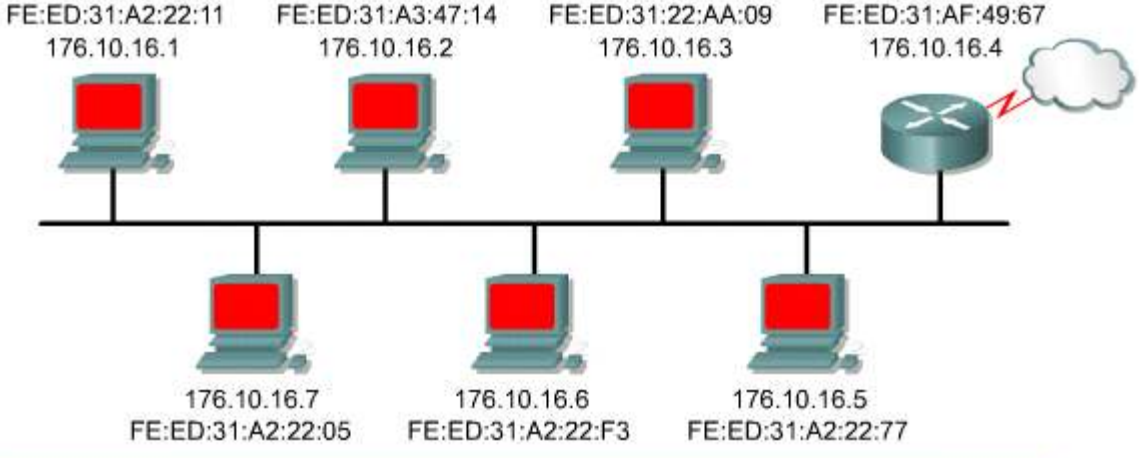


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

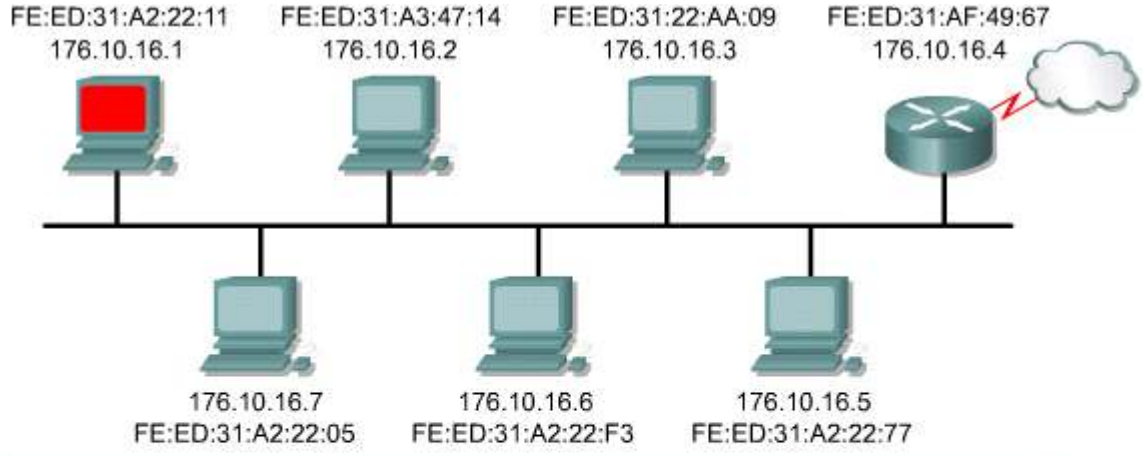


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

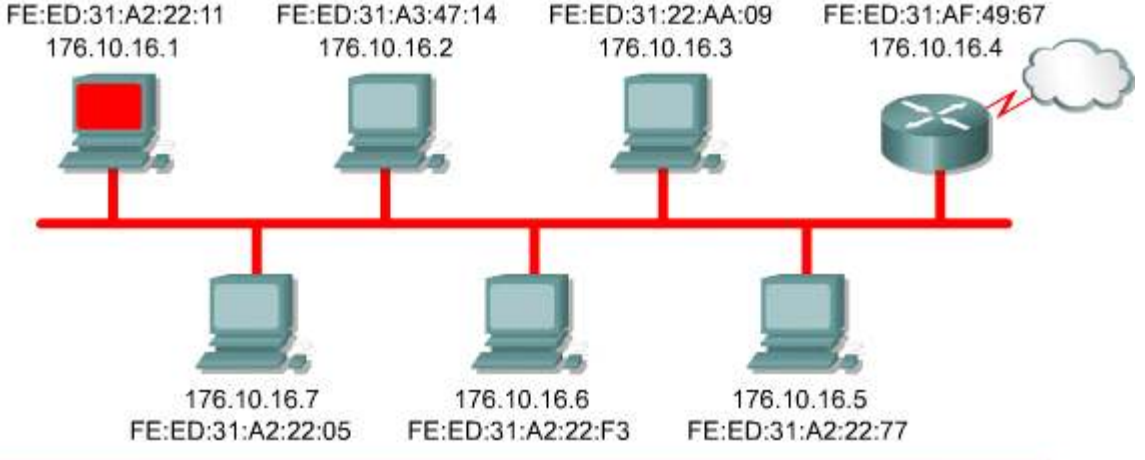


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

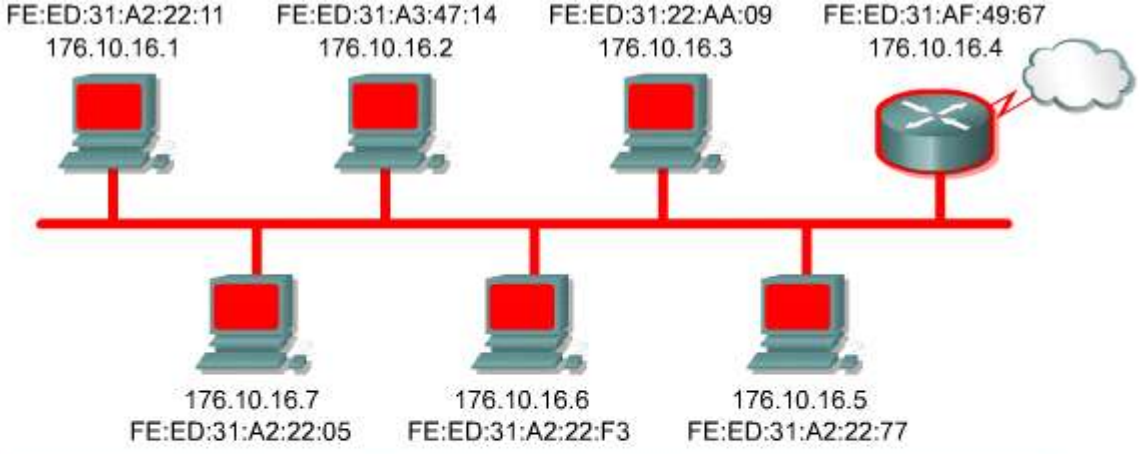


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

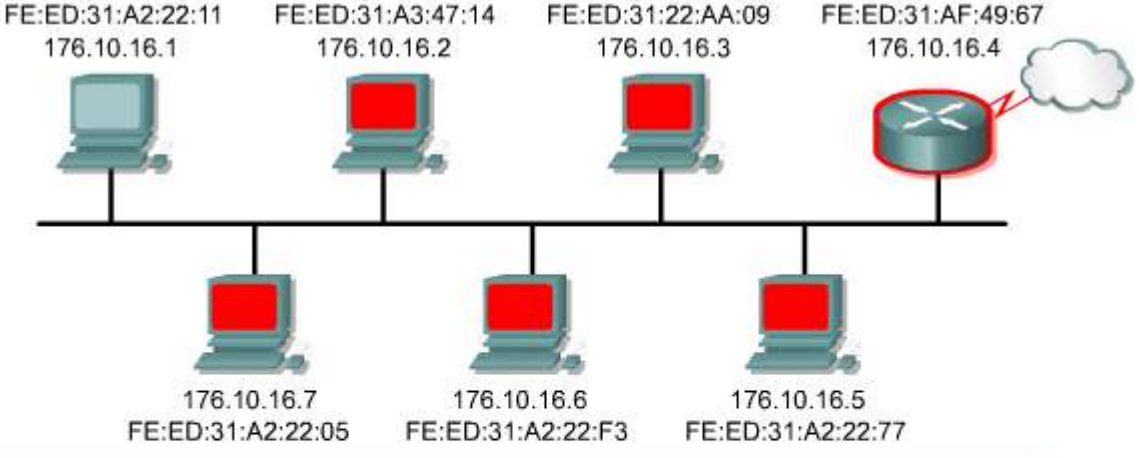


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

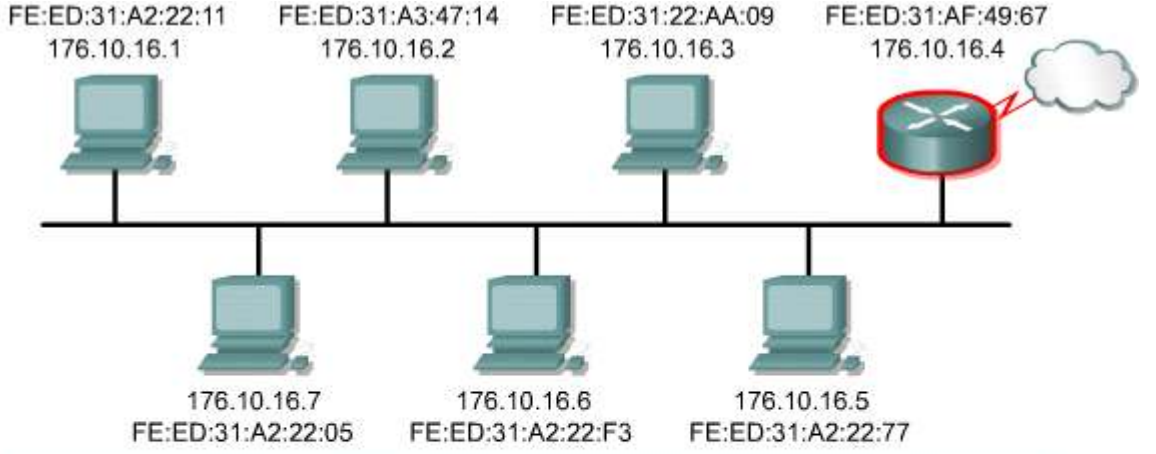


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.4	FE:ED:31:AF:49:67

Proxy ARP est une variante du protocole ARP. Dans cette variante, un routeur envoie une réponse ARP, qui contient l'adresse MAC de l'interface qui a reçu la requête, à l'hôte demandeur. Le routeur répond avec ses adresses MAC aux requêtes dont l'adresse IP n'appartient pas à la plage d'adresses du sous-réseau local.

Une autre solution pour envoyer des données à l'adresse d'un équipement situé sur un autre segment du réseau, consiste à configurer une passerelle par défaut. 6

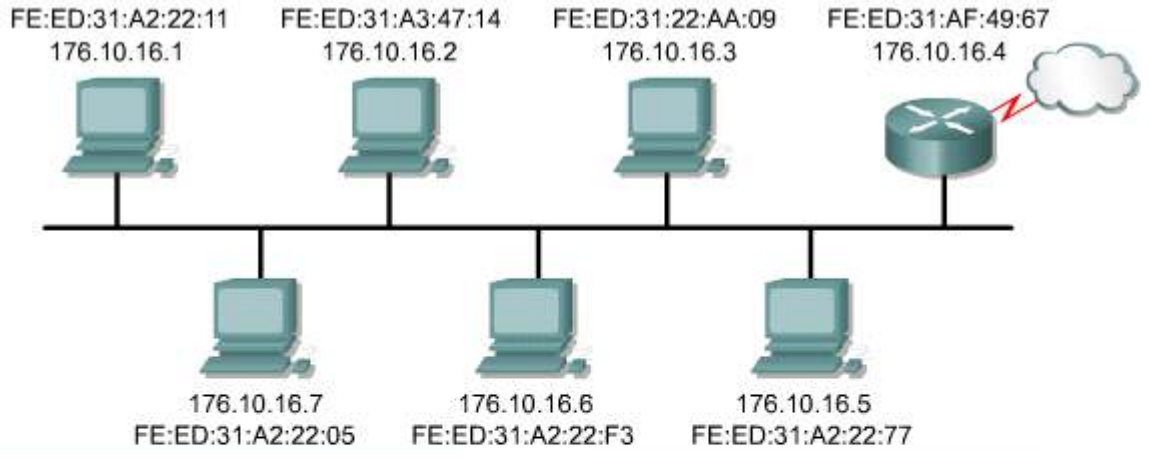


Table ARP

Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut

176.10.16.4	FE:ED:31:AF:49:67

Fenêtre contextuelle (pop up)

L'ordinateur 176.10.16.1 doit transmettre des données à l'ordinateur 199.11.20.5 l'adresse MAC de la passerelle par défaut.

L'ordinateur 176.10.16.1 prépare les données à transmettre à l'ordinateur 199.11.20.5. Lors de l'élaboration de la trame pour la transmission, il constate que la paire IP-MAC de l'ordinateur 199.11.20.5 ne se trouve pas dans sa table ARP. Lorsque la passerelle par défaut est définie sur cet ordinateur, l'adresse de destination est comparée à l'adresse source des hôtes. Cette opération révèle que l'adresse de destination est située sur un autre réseau. L'hôte élabore alors la trame des données à l'aide de l'adresse IP de destination et de l'adresse MAC des passerelles par défaut.

L'ordinateur 176.10.16.1 transmet les trames de données via le segment du câble réseau.

Tous les hôtes du même segment analysent les trames entrantes.

Tous les ordinateurs, à l'exception du routeur 176.10.16.4, ignorent les trames, car ces dernières ne correspondent pas à l'adresse MAC de destination des trames entrantes.

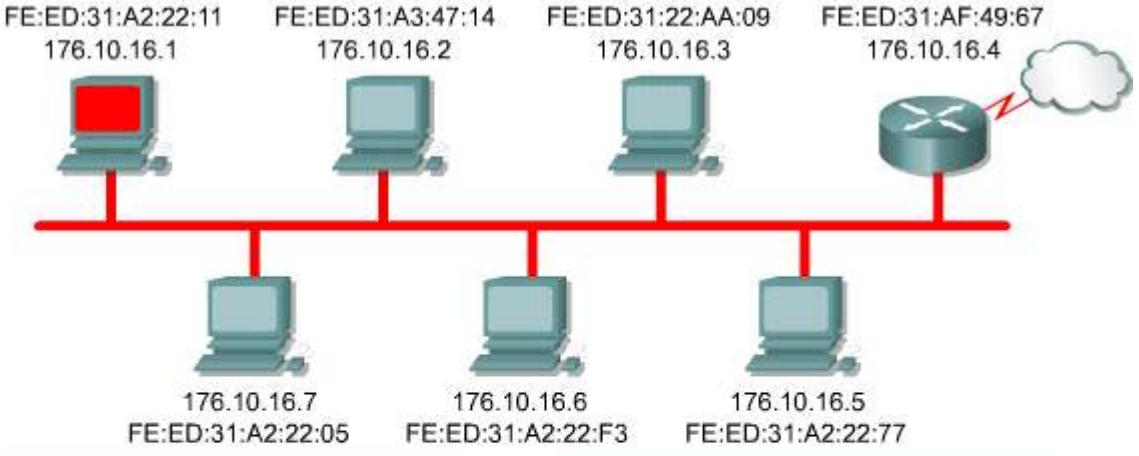


Table ARP	
Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut	
176.10.16.4	FE:ED:31:AF:49:67

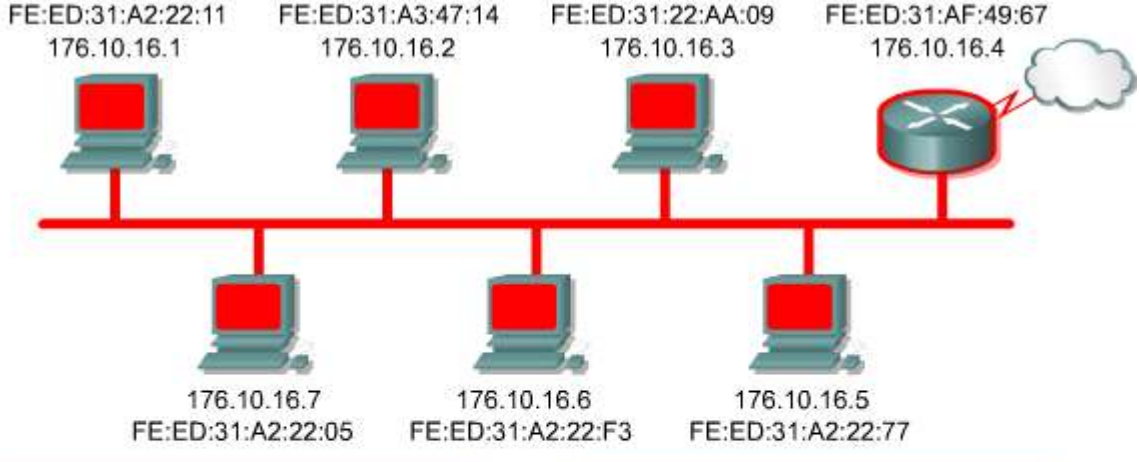


Table ARP	
Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut	
176.10.16.4	FE:ED:31:AF:49:67

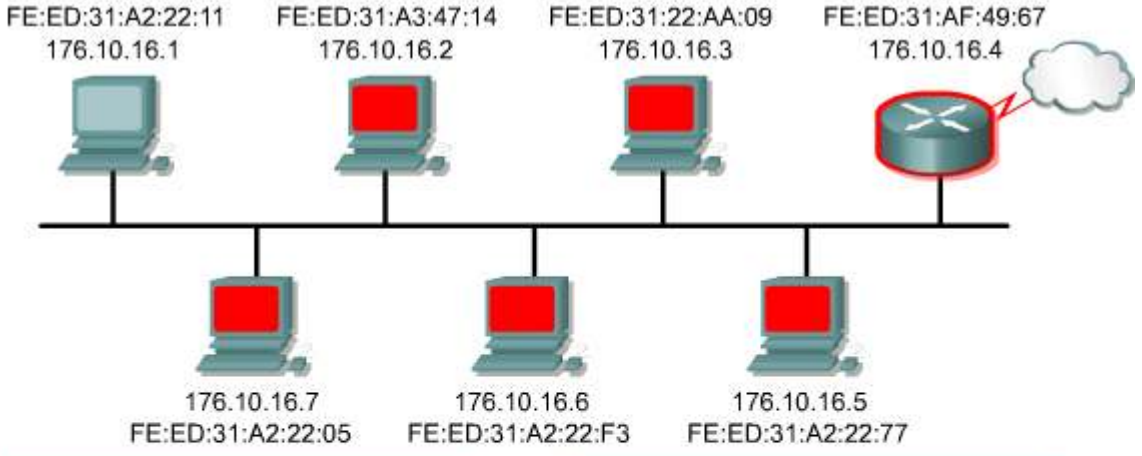


Table ARP	
Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut	
176.10.16.4	FE:ED:31:AF:49:67

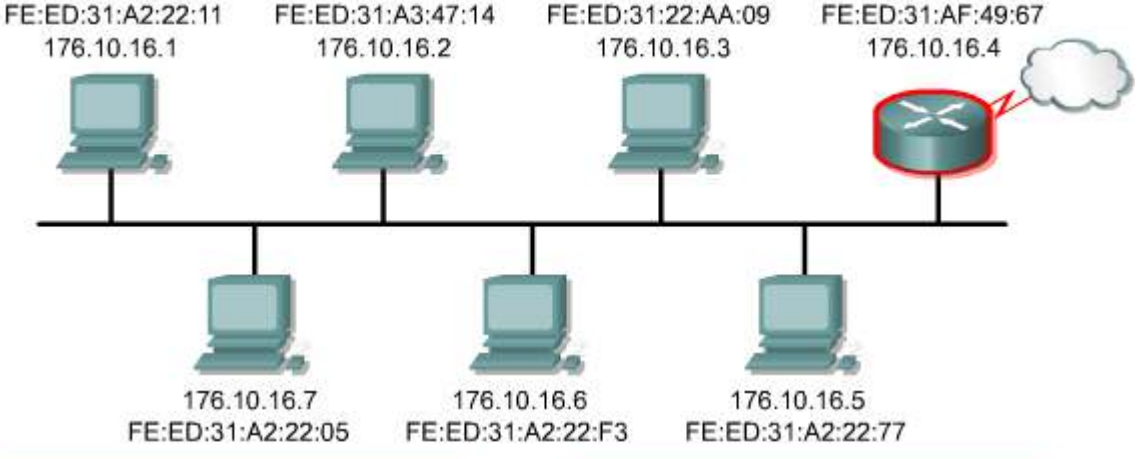


Table ARP	
Adresse IP	Adresse MAC
176.10.16.3	FE:ED:31:22:AA:09
176.10.16.6	FE:ED:31:A2:22:F3
176.10.16.5	FE:ED:31:A2:22:77
176.10.16.2	FE:ED:31:A3:47:14
176.10.16.2	FE:ED:31:A3:47:14

Passerelle par défaut	
176.10.16.4	FE:ED:31:AF:49:67

Une passerelle par défaut est une option « host » dans laquelle l'adresse IP de l'interface du routeur est enregistrée dans la configuration réseau de l'hôte. L'hôte source compare l'adresse IP de destination à sa propre adresse IP afin de déterminer si les deux adresses sont situées sur le même segment. Si l'hôte de destination ne se trouve pas sur le même segment, l'hôte d'origine envoie les données en utilisant l'adresse IP actuelle de

destination et l'adresse MAC du routeur. Cette dernière a été extraite de la table ARP à l'aide de l'adresse IP du routeur.

Si la passerelle par défaut de l'hôte ou la fonction Proxy ARP du routeur n'est pas configurée, aucune donnée ne peut quitter le réseau local. L'une ou l'autre est nécessaire pour établir une connexion avec une machine située à l'extérieur du réseau local.

L'activité de TP présente la commande **arp -a**.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux appréhender le processus ARP.

Cette page termine la leçon. La page suivante récapitule les principaux points évoqués au cours de ce module.



Activité de TP

Exercice: Protocole ARP de la station de travail ARP

L'objectif de ce TP est de présenter le protocole de résolution d'adresse (ARP) et la commande **arp -a** sur une station de travail.



Activité de média interactive

Glisser-Positionner: Processus ARP

À l'issue de cette activité, les étudiants seront capables d'identifier les différents processus ARP.

Résumé

Cette page résume les sujets traités dans ce module.

Le modèle de référence TCP/IP développé par le ministère américain de la défense (*DoD*) comporte quatre couches : la couche application, la couche transport, la couche Internet et la couche d'accès au réseau. La couche application gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. La couche transport offre des services de transport de l'hôte à la destination. Le rôle de la couche Internet consiste à sélectionner le meilleur chemin pour transmettre les paquets sur le réseau. La couche d'accès au réseau est responsable de l'établissement d'une liaison physique à un support réseau.

Bien que certaines couches du modèle de référence TCP/IP correspondent aux sept couches du modèle OSI, des différences existent. Le modèle TCP/IP intègre la couche présentation et la couche session dans sa couche application. Le modèle TCP/IP regroupe les couches physique et liaison de données du modèle OSI dans sa couche d'accès au réseau.

Les routeurs utilisent l'adresse IP pour acheminer les paquets de données d'un réseau à un autre. Les adresses IP ont une longueur de trente deux bits (dans la version 4 du protocole IP) et sont divisées en quatre octets de huit bits. Ils fonctionnent au niveau de la couche réseau (couche 3) du modèle OSI, qui est la couche Internet du modèle TCP/IP.

L'adresse IP d'un hôte est une « adresse logique », ce qui signifie qu'elle peut être modifiée. L'adresse MAC (*Media Access Control*) de la station de travail est une adresse physique de 48 bits. Elle est généralement inscrite de manière indélébile sur la carte réseau. La seule façon de la modifier est de remplacer la carte réseau. Afin de transmettre des données TCP/IP dans un segment LAN, une adresse IP de destination et une adresse MAC de destination sont requises. Bien que l'adresse IP soit unique et routable sur Internet, elle doit

pouvoir être mappée avec une adresse MAC lors de la réception d'un paquet sur le réseau de destination. La pile de protocoles TCP/IP comprend un protocole appelé «ARP» (*Address Resolution Protocol*) qui peut obtenir automatiquement les adresses MAC pour la transmission locale. Une variante du protocole ARP, appelée « Proxy ARP », fournit l'adresse MAC d'un équipement intermédiaire pour la transmission de données à un autre segment du réseau.

Il existe cinq classes d'adresses IP (de A à E). Seules les trois premières classes sont utilisées commercialement. En fonction de la classe, les parties réseau et hôte de l'adresse occupent un nombre différent de bits. Les adresses de classe D sont utilisées pour les groupes de multicast. Les adresses de classe E sont utilisées à des fins expérimentales.

Une adresse IP dont tous les bits hôte sont occupés par des 0 binaires est utilisée pour identifier le réseau lui-même. Une adresse dont tous les bits hôte sont occupés par des 1 correspond à une adresse de broadcast. Elle est utilisée pour diffuser des paquets vers tous les équipements d'un réseau.

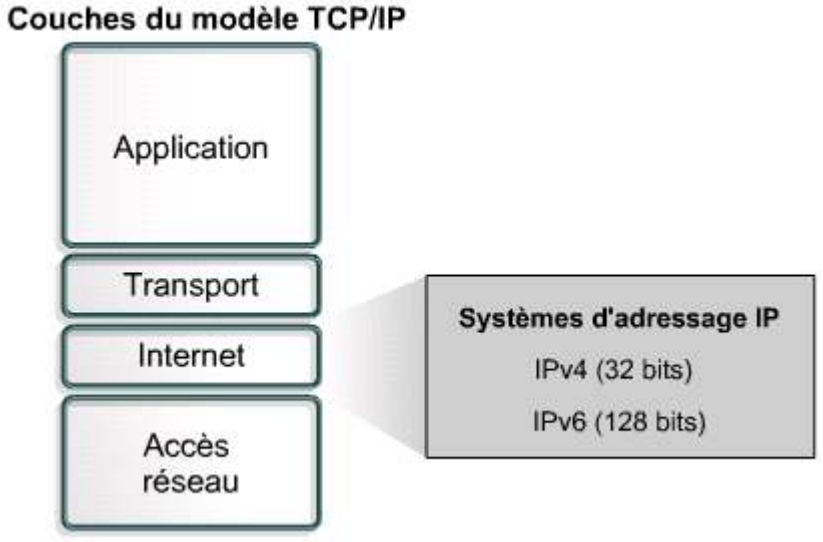
Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique. Les adresses IP publiques sont mondiales et normalisées. Les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse hôte, dès lors que chacun des hôtes du réseau privé est unique. Trois blocs d'adresses IP sont réservés pour une utilisation privée et interne. Ces blocs se composent d'une classe A, d'une plage d'adresses de classe B et d'une plage d'adresses de classe C. Toutes les adresses appartenant à ces plages sont rejetées par les routeurs et ne sont pas acheminées sur le backbone d'Internet.

Le découpage en sous-réseaux représente une solution de rechange pour subdiviser un LAN et y identifier des réseaux distincts. La subdivision d'un réseau en sous-réseaux implique l'utilisation du masque de sous-réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces. Les adresses de sous-réseau contiennent une partie réseau, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine pour l'ensemble du réseau.

Une version encore plus flexible et évolutive de la norme IP (IPv6) a fait son apparition. Il s'agit d'IPv6 qui encode les adresses sur 128 bits au lieu de 32 (en utilisant des nombres hexadécimaux). Le protocole IPv6 s'implante sur certains réseaux et devrait finir par supplanter le protocole IPv4.

Les adresses IP sont attribuées aux hôtes comme suit:

- **De façon statique** (manuellement) – par l'administrateur réseau.
- **De façon dynamique** (automatiquement) – à l'aide des protocoles RARP, BOOTP ou DHCP.



10-Notions de bases sur le routage et les sous-réseaux

Vue d'ensemble

Le protocole IP (*Internet Protocol*) est le principal protocole routé d'Internet. Les adresses IP permettent d'acheminer les paquets depuis une source vers une destination en empruntant le meilleur chemin possible. La propagation des paquets, les modifications de l'encapsulation et les protocoles orientés et non orientés connexion sont également essentiels à la bonne livraison des données. Ce module présente chacun de ces éléments.

La différence entre les protocoles de routage et les protocoles routés est souvent source de confusion. Les deux concepts, bien que similaires en apparence, sont en fait très différents. Les routeurs se servent des protocoles de routage pour créer les tables qui leur permettront de déterminer le meilleur chemin vers un hôte sur Internet.

Les organisations ne peuvent pas toutes être classées dans les trois classes d'adresses (A, B et C). La subdivision en sous-réseaux apporte de la flexibilité à ce système de classes. Elle permet aux administrateurs réseau de déterminer la taille du réseau dont ils auront besoin. Une fois qu'ils ont choisi le type de segmentation de leurs réseaux, ils emploient des masques de sous-réseau pour définir l'emplacement de chacune des machines sur le réseau.

Ce module se rapporte à des objectifs spécifiques des examens de certification CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP afin de répondre aux exigences de conception • Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs • Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco	• Mise en œuvre d'un LAN		

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Établissement d'un système d'adressage IP pour la prise en charge de l'adressage par classe, sans classe et privé afin de répondre aux exigences de conception. • Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Mise en œuvre d'un LAN		• Évaluation des caractéristiques des protocoles de routage • Évaluation des règles de gestion des paquets

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Utilisation des techniques d'adressage IP • Description des principes et de l'usage de la commutation de paquets utilisant le protocole IP (Internet Protocol) • Description des concepts associés au routage, ainsi que des différents protocoles et méthodes visant à sa réalisation • Description du mode d'association entre une adresse IP et l'interface d'une unité, et de l'association entre les techniques d'adressage

À l'issue de ce module, les étudiants seront en mesure d'effectuer les actions suivantes: 1

	À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :
10.1	Protocole routé
10.2	Protocoles de routage IP
10.3	Mécanisme de découpage en sous-réseaux

- Décrire les protocoles routés.
- Énumérer les étapes de l'encapsulation des données dans un interréseau lors de leur acheminement vers les unités de couche 3.
- Décrire la transmission orientée connexion et la transmission non orientée connexion.
- Énumérer les champs d'un paquet IP.
- Expliquer comment les données sont acheminées.
- Comparer les différents types de protocoles de routage.
- Énumérer et décrire plusieurs des métriques utilisées par les protocoles de routage.
- Dresser la liste des différentes utilisations d'un sous-réseau.
- Déterminer le masque de sous-réseau pour une situation donnée.
- Utiliser le masque de sous-réseau pour déterminer l'adresse de sous-réseau.

10.1 Protocole routé

10.1.1 Protocole routé et protocole routable

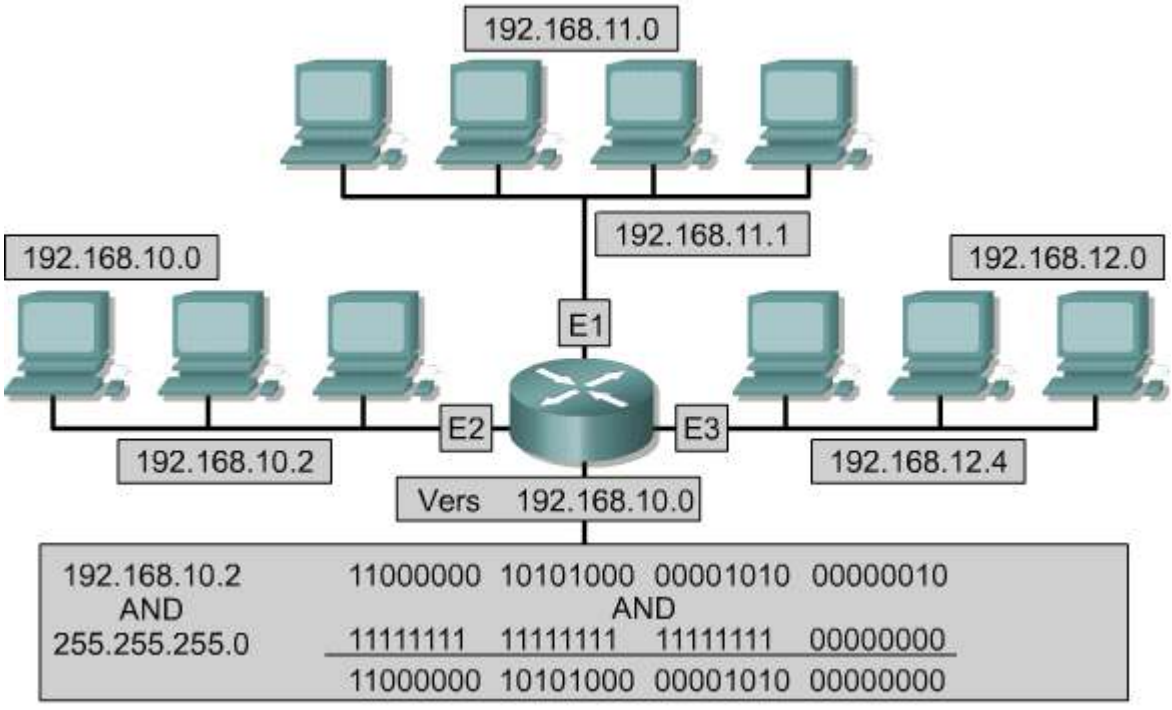
Cette page explique ce que sont les protocoles routés et les protocoles routables.

Un protocole est un ensemble de règles qui définit le mode de communication entre les différents ordinateurs sur les réseaux. Pour communiquer entre eux, les ordinateurs échangent des messages. Afin de pouvoir accepter et traiter ces messages, il leur faut disposer d'ensembles de règles qui déterminent la manière de les interpréter. Les messages utilisés pour établir une connexion avec une machine distante, les messages électroniques et les fichiers transférés sur un réseau sont autant d'exemples de ces messages.

Un protocole décrit les éléments suivants:

- Le format de message requis.
- La manière dont les ordinateurs doivent échanger les messages d'activités spécifiques.

Un protocole routé permet au routeur de transmettre des données entre les nœuds de différents réseaux. 1



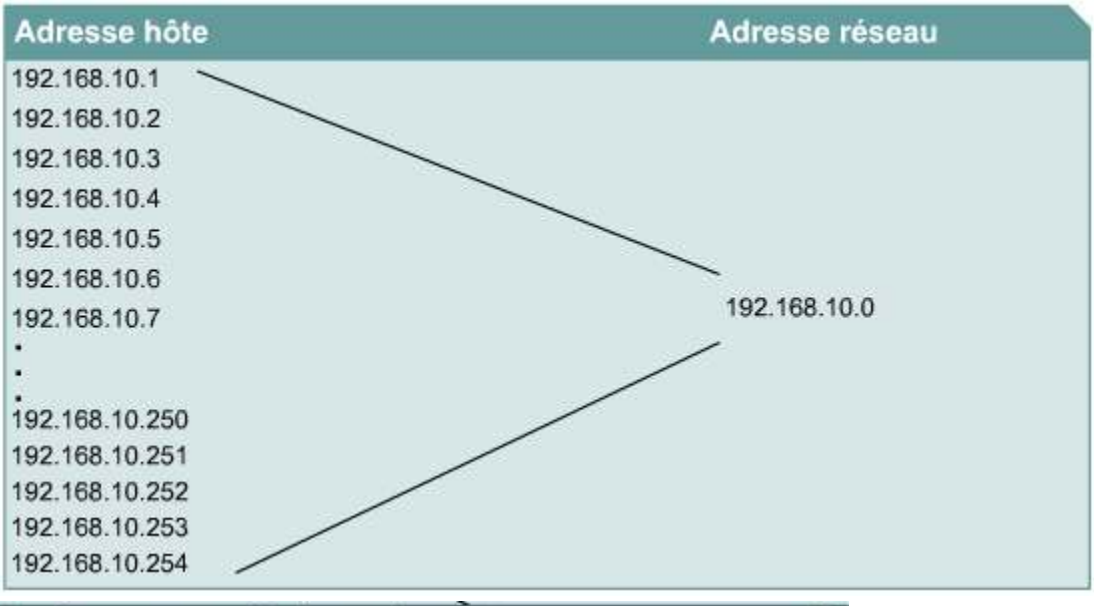
Fenêtre contextuelle (pop up)

Un réseau comporte une adresse hôte IP et une adresse réseau. Les deux sont nécessaires pour un réseau routé. Un masque de réseau permet de séparer les parties réseau et hôte d'une adresse IP de 32 bits. L'opération AND crée une adresse réseau qui identifie une interface spécifique. Les données doivent être acheminées vers cette interface pour atteindre le réseau de destination.

Un protocole routable doit impérativement permettre d'attribuer un numéro de réseau et un numéro d'hôte à chacune des machines. Certains protocoles, à l'instar du protocole IPX, ne requièrent que le numéro de réseau. Ils utilisent alors l'adresse MAC de l'hôte à la place de son numéro. D'autres protocoles, comme IP, nécessitent que l'adresse comporte une partie réseau et une partie hôte. Dans ce cas, un masque de réseau est nécessaire

pour différencier ces deux numéros. L'adresse réseau est ensuite obtenue en effectuant une opération AND logique sur l'adresse et le masque de réseau.

L'objectif du masque de réseau est de permettre à des groupes d'adresses IP séquentielles d'être traités en tant qu'une seule et même unité. 2



Fenêtre contextuelle (pop up)

L'ensemble des 254 adresses comprises dans la séquence allant de 192.168.10.1 à 192.168.10.254 peuvent être représentées par l'adresse réseau 192.168.10.0. Grâce à cette adresse réseau, les données peuvent être envoyées vers n'importe lequel de ces hôtes. Il n'est pas nécessaire que les tables de routage contiennent les 254 adresses, une seule suffit : l'adresse 192.168.10.0.

Sans ce regroupement, chaque hôte devrait être mappé individuellement pour le routage, ce qui est impossible à réaliser. En effet, selon le consortium ISC (*Internet Software Consortium*), il existerait quelque 233 101 500 hôtes sur Internet.

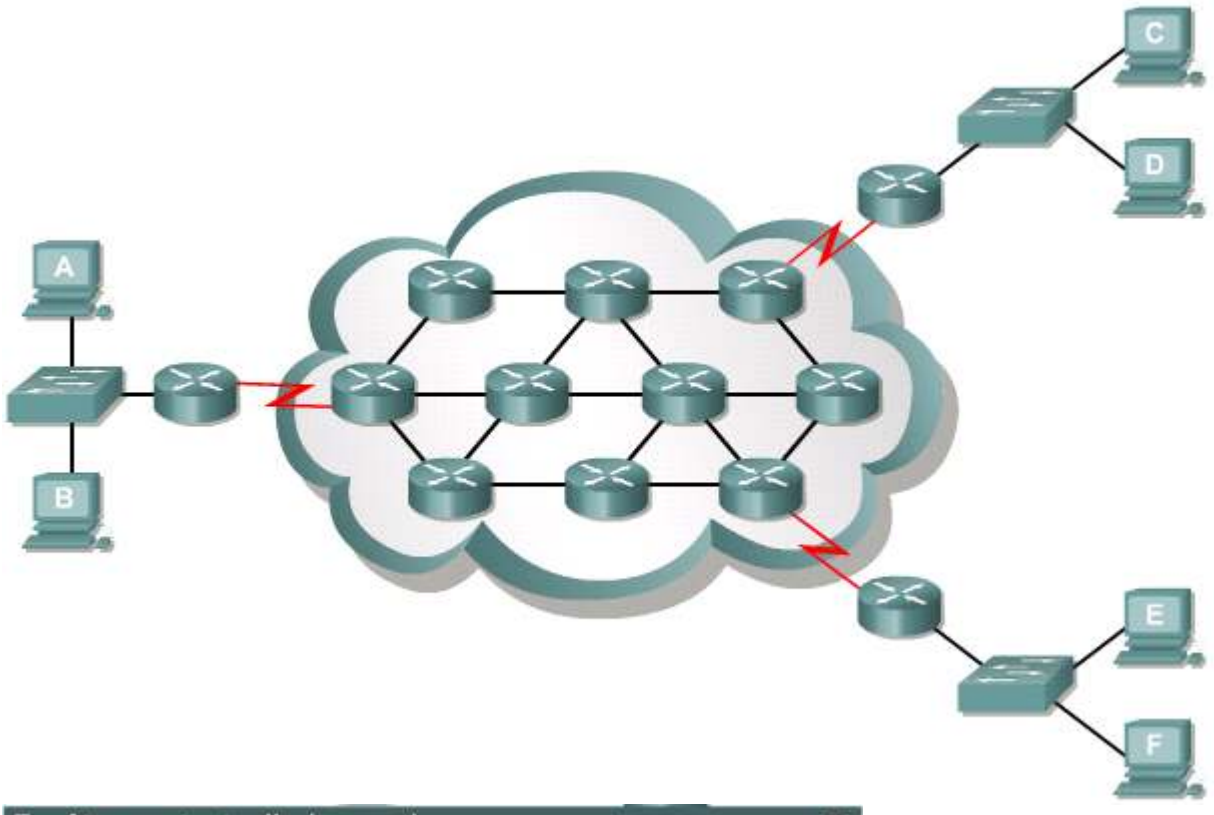
La page suivante aborde le protocole IP.

10.1 Protocole routé

10.1.2 IP comme protocole routé

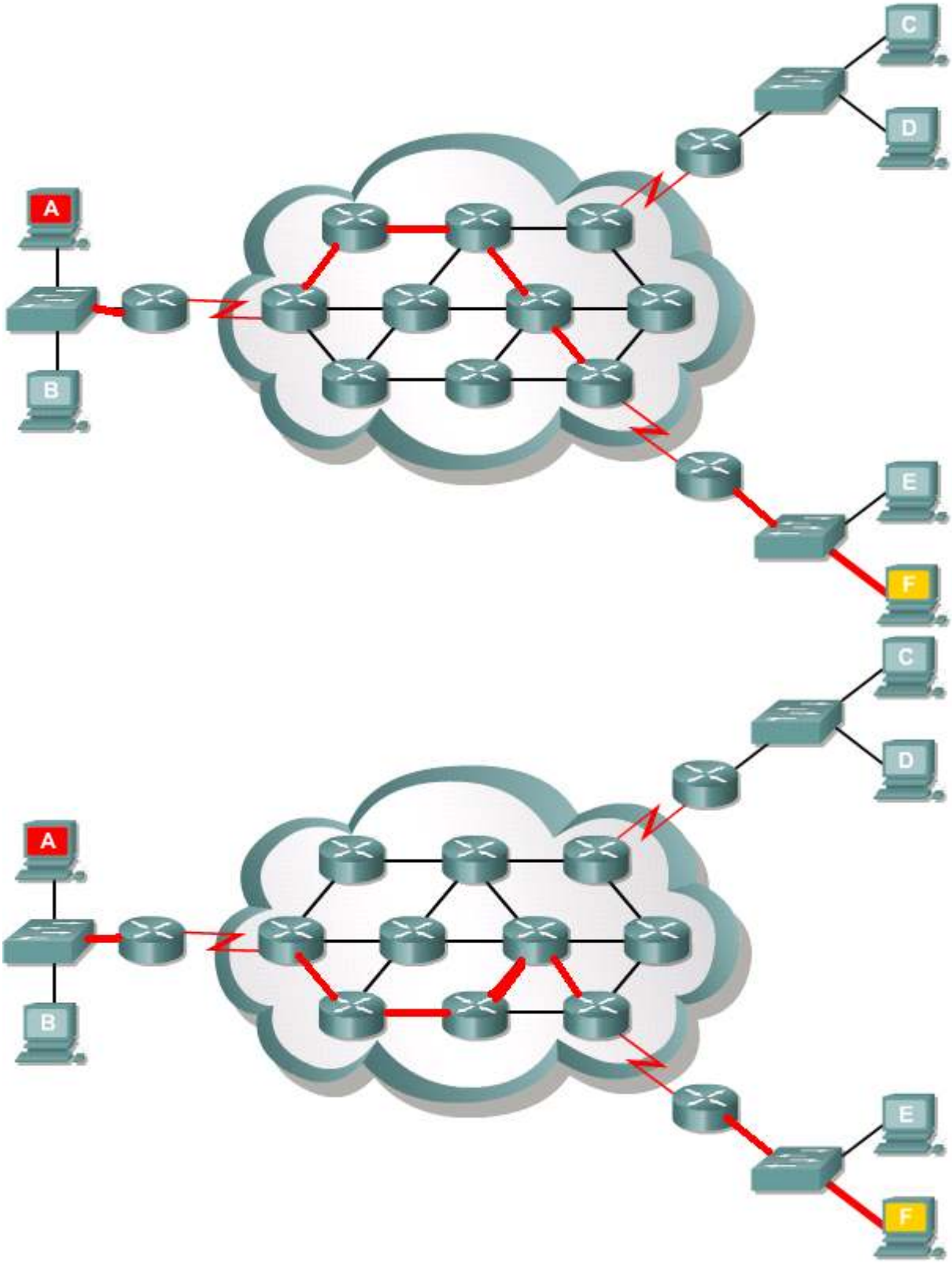
Cette page décrit les caractéristiques et les fonctions du protocole IP.

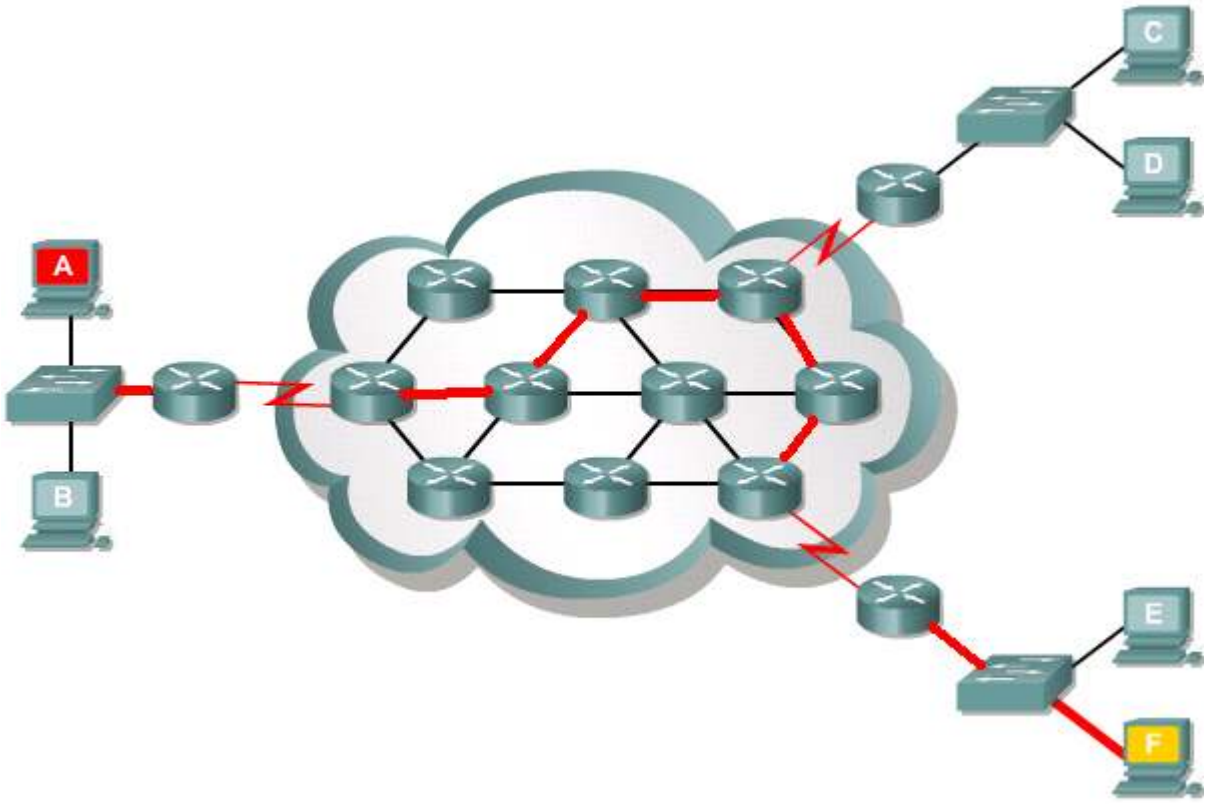
IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé. C'est un protocole non orienté connexion, peu fiable et axé sur l'acheminement au mieux (best-effort delivery). Le terme «non orienté connexion» signifie qu'aucune connexion à un circuit dédié n'est établie avant la transmission. Le protocole IP détermine le meilleur chemin pour les données en fonction du protocole de routage. Les termes «peu fiable» et «au mieux» ne signifient pas que le système n'est pas fiable et qu'il fonctionne mal, mais plutôt que le protocole IP ne s'assure pas de la bonne livraison des données envoyées sur le réseau. Si cette vérification est nécessaire, elle est effectuée par les protocoles de couche supérieure. 1



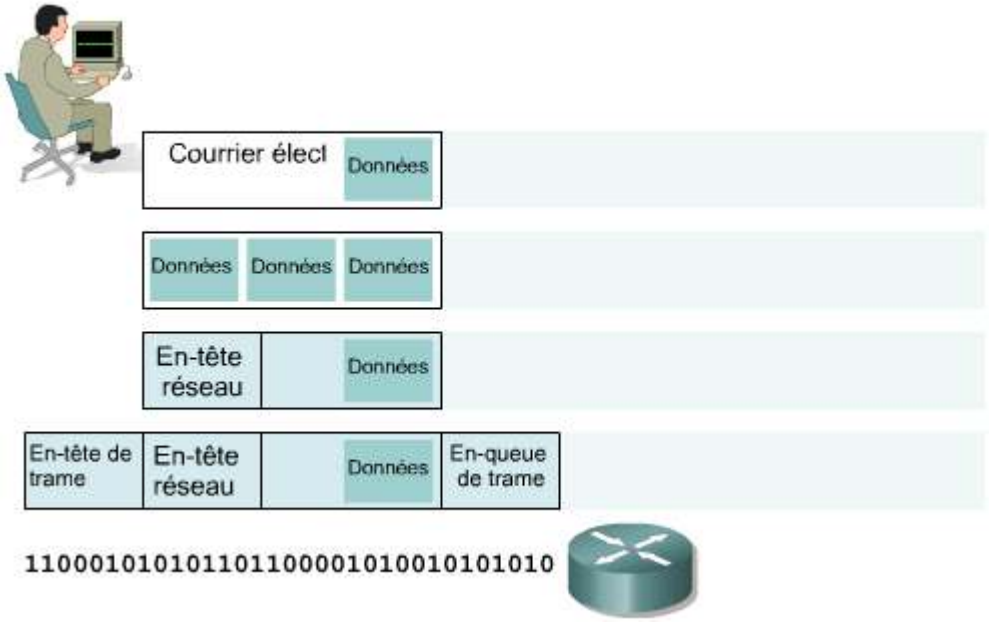
Fenêtre contextuelle (pop up)

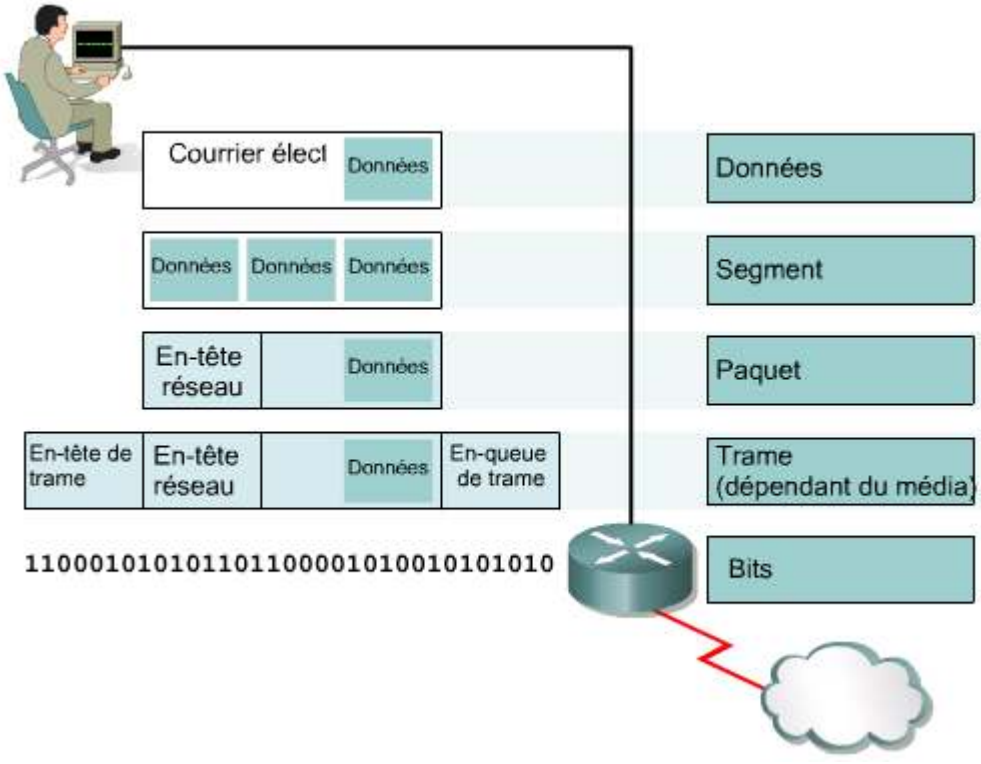
Le protocole IP choisit le chemin le plus efficace en fonction de la décision du protocole de routage.
Si l'ordinateur A envoyait des données à l'ordinateur F, quel chemin ces dernières prendraient-elles ? Ce sont les routeurs qui font ce choix, à l'aide des protocoles de routage.


A
B
C
D
E
F
A
B
C
D
E
F

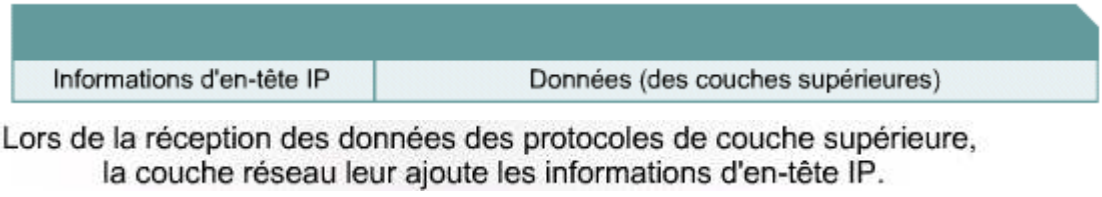


Les données sont traitées au niveau de chaque couche du modèle OSI au fur et à mesure qu'elles circulent vers le bas du modèle. 2





Au niveau de la couche réseau, les données sont encapsulées dans des paquets. Ces paquets sont appelés des datagrammes. 3


Informations d'en-tête IP
Données (des couches supérieures)
Lors de la réception des données des protocoles de couche supérieure, la couche réseau leur ajoute les informations d'en-tête IP.

IP détermine le contenu de l'en-tête du paquet IP, qui contient les informations d'adressage. Il ne se préoccupe toutefois pas des données proprement dites. Il se contente de les accepter lorsqu'il les reçoit des couches supérieures.

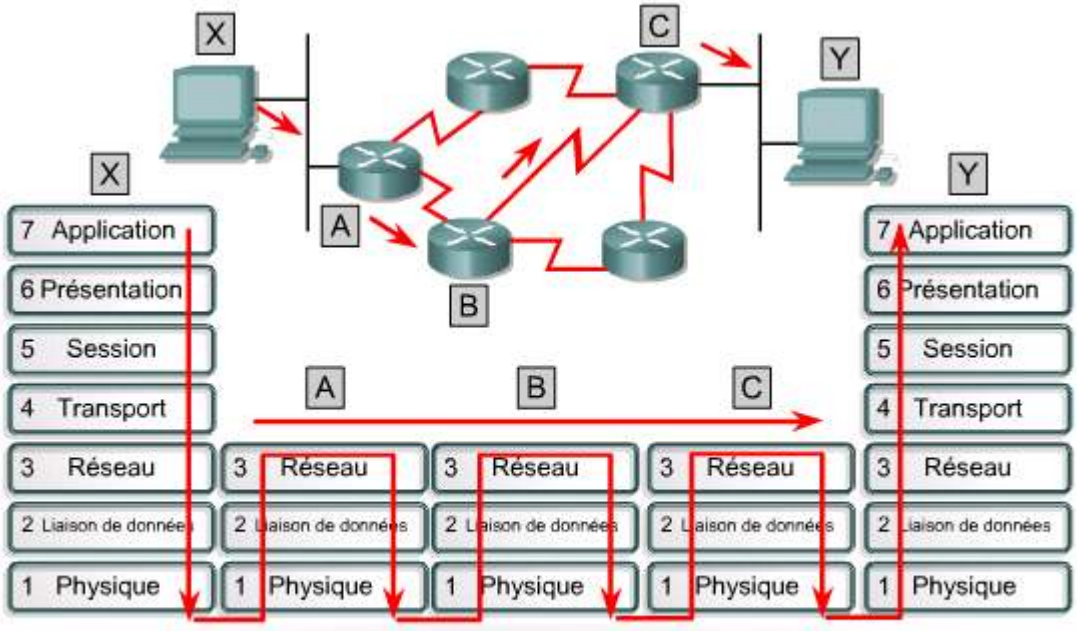
La page suivante examine l'acheminement d'un paquet sur un réseau.

10.1 Protocole routé

10.1.3 Propagation d'un paquet et commutation au sein d'un routeur

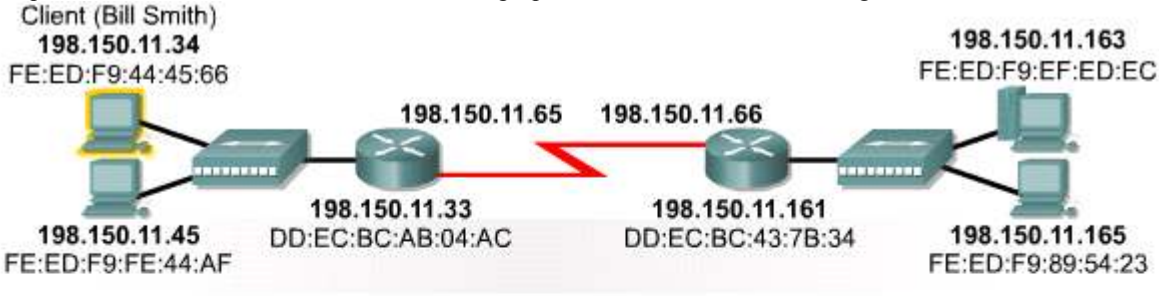
Cette page explique ce qui se passe lorsqu'un paquet circule sur un réseau.

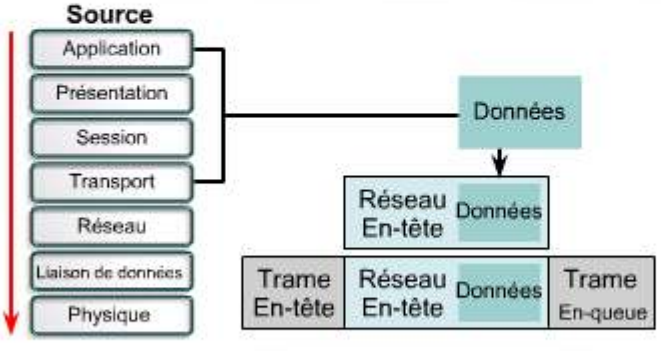
Au cours de l'acheminement d'un paquet sur un interréseau jusqu'à sa destination finale, les en-queues et les en-têtes de trame de la couche 2 sont retirés et remplacés au niveau de chacune des unités de couche 3. 1



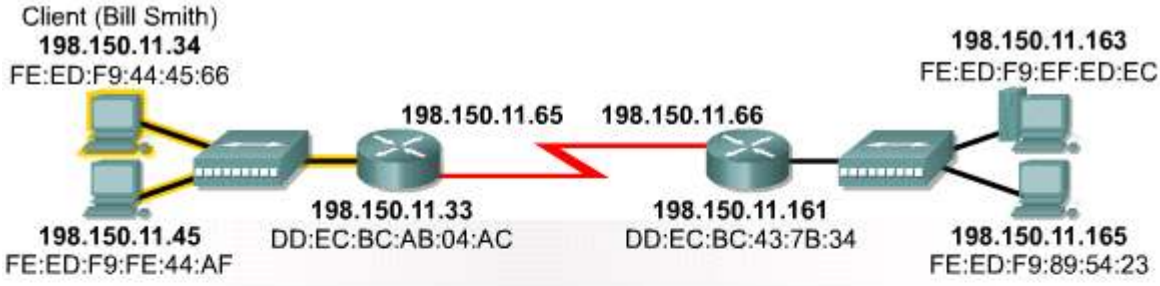
Chaque routeur fournit ses services pour la prise en charge des fonctions de la couche supérieure.

Cela s'explique par le fait que les unités de données de la couche 2, ou trames, sont destinées à l'adressage local, tandis que les unités de données de la couche 3, ou paquets, sont destinées à l'adressage de bout en bout. 2



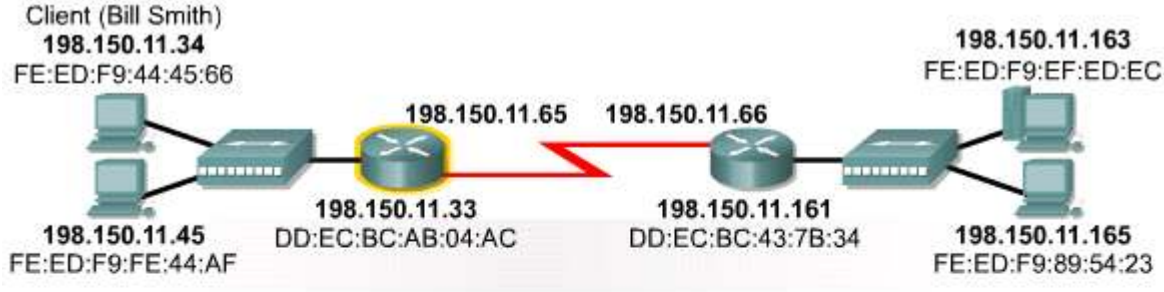


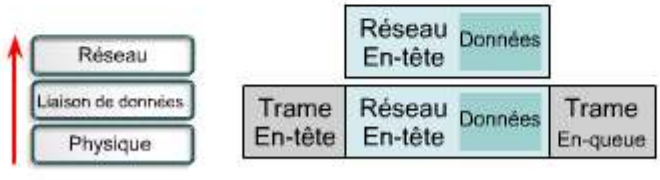
La couche transport segmente, séquence et ajoute le contrôle d'erreur au message électronique. Les adresses source et de destination de la couche réseau sont ajoutées au datagramme. Le cache ARP fournit l'adresse MAC correspondant à l'adresse IP de destination. Ainsi, la trame Ethernet est ajoutée et comprend les adresses source et de destination.



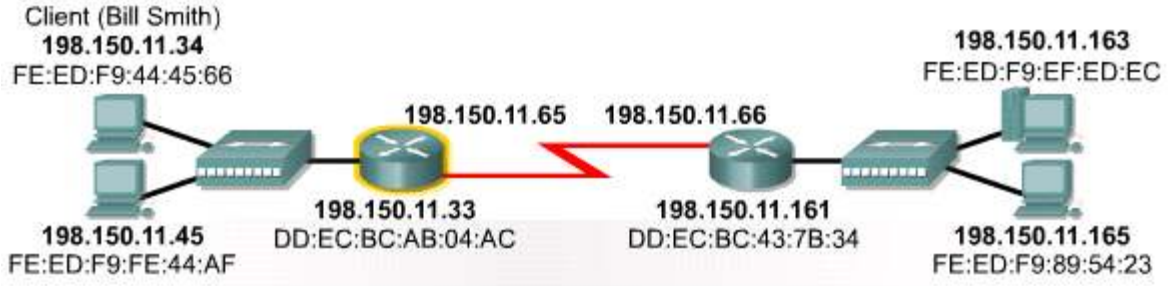
Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	Source	Source	Destination		
DD:EC:BC:AB:04:AC	FE:ED:F9:44:45:66	198.150.11.34	198.150.11.163	Courrier électronique Données	CRC-32

Les trames de données sont ensuite transmises sur le segment Ethernet. Toutes les stations de travail prennent la trame et vérifient si elle leur est destinée. Toutes les unités, à l'exception du routeur, rejettent la trame.



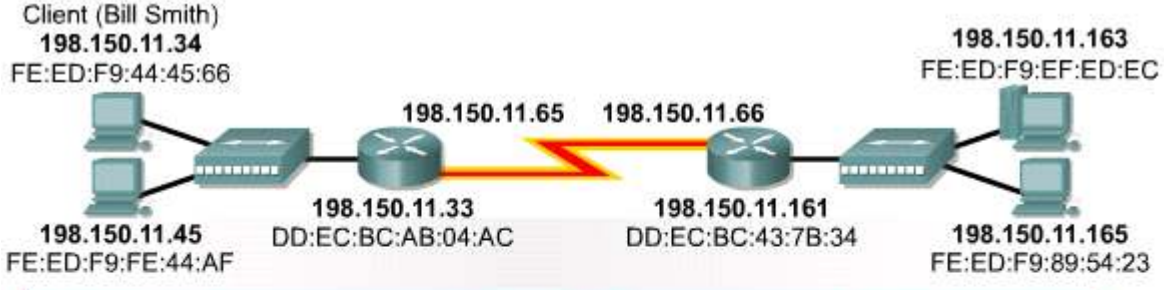


Le routeur récupère la trame qui était adressée à son adresse MAC et retire la trame Ethernet.

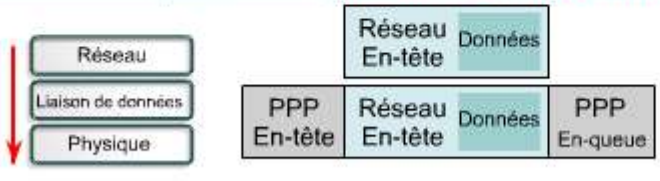


198.150. 11.163	**Adresse IP**
255.255.255.224	**Masque de sous-réseau**
198.150. 11.160	**Résultat**

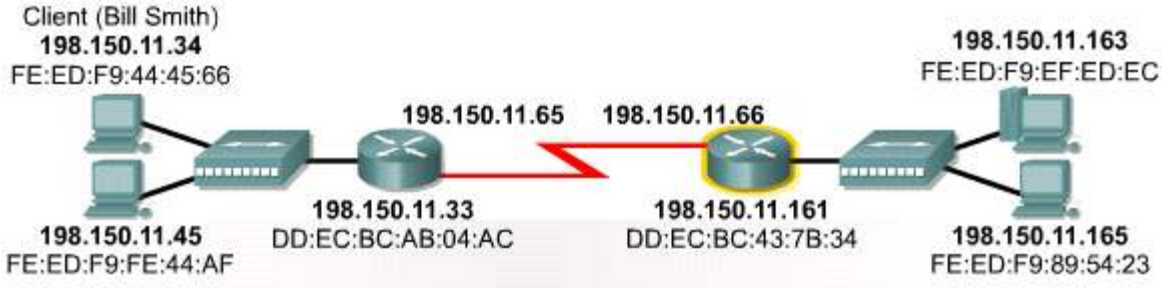
Le routeur applique le masque de sous-réseau à l'adresse de destination. Il compare ensuite le résultat avec sa table de routage. La table indique que pour accéder au réseau 198.150.11.160, le paquet doit être transmis au port série,

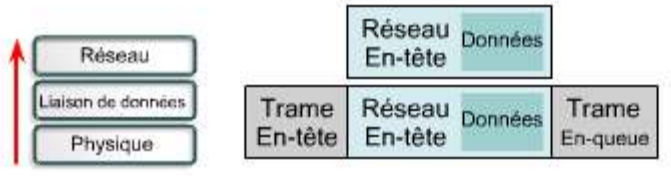


Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	**Source**	**Source**	**Destination**		
PPP	PPP	198.150.11.34	198.150.11.163	Courrier électronique	CRC-32

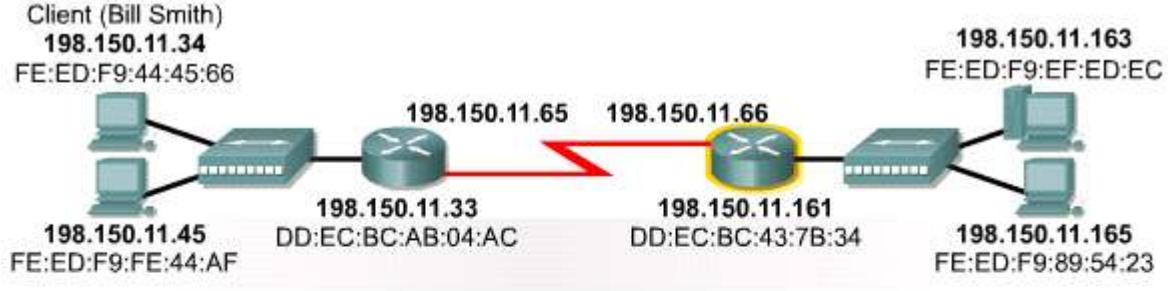


La demande est encapsulée pour une transmission série, puis envoyée au routeur



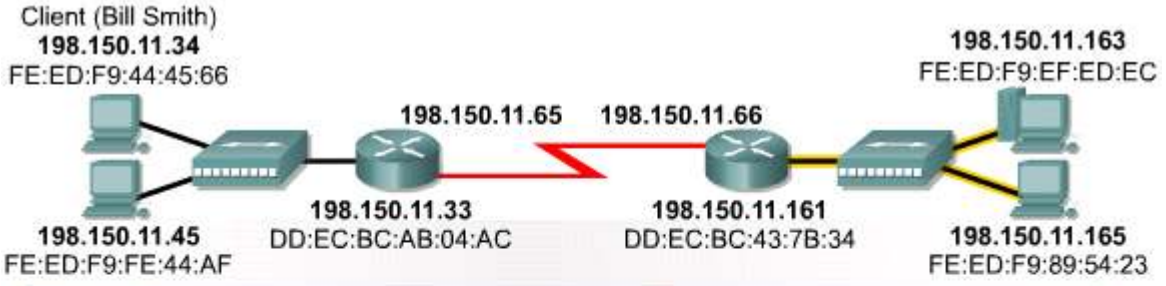


Le routeur récupère la trame et retire la trame PPP.

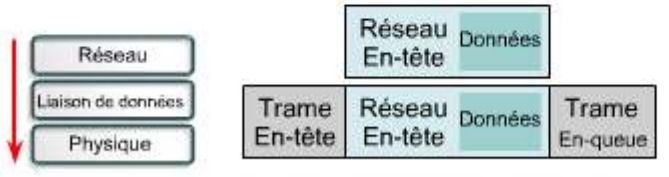


198.150. 11.163	**Adresse IP**
255.255.255.224	**Masque de sous-réseau**
198.150. 11.160	**Résultat**

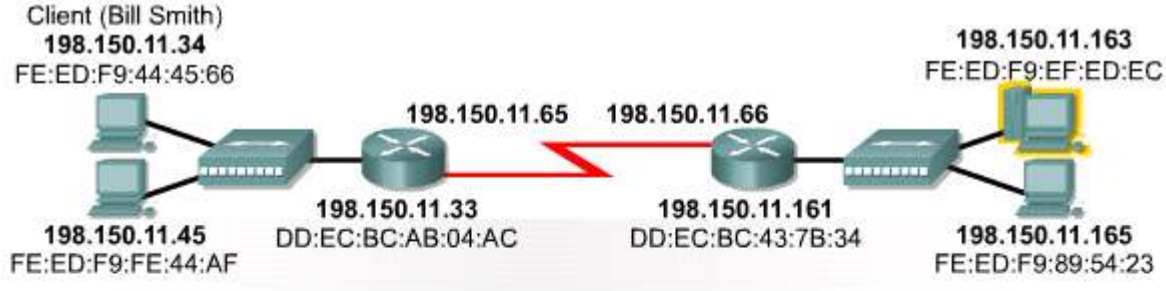
Le routeur applique le masque de sous-réseau à l'adresse de destination. Il compare ensuite le résultat avec sa table de routage. La table indique que pour accéder au réseau 198.150.11.160, le paquet doit être transmis au port Ethernet, 198.150.11.161, sur le routeur.

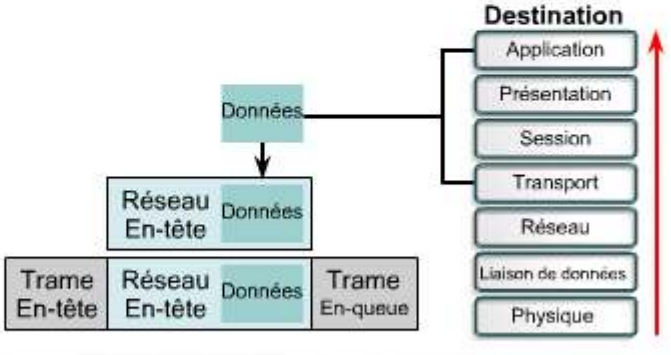


Trame En-tête		Réseau En-tête		Données	Trame En-queue
Destination	Source	Source	Destination		
FE:ED:F9:EF:ED:EC	DD:EC:BC:43:7B:34	198.150.11.34	198.150.11.163	Courrier électronique	CRC-32



La demande est encapsulée pour la transmission Ethernet et envoyée sur le segment Ethernet. Toutes les stations de travail prennent la trame et vérifient si elle leur est destinée. Toutes les unités, à l'exception de l'ordinateur doté





L'ordinateur récepteur désencapsule le paquet et traite les données. Cela signifie que la couche transport réassemble les paquets de données dans l'ordre approprié et recherche les erreurs éventuelles.

Les trames Ethernet de la couche 2 sont conçues pour circuler au sein d'un domaine de broadcast grâce à l'adresse MAC gravée sur le matériel. Les autres types de trames de la couche 2 comprennent les liaisons série PPP et les connexions Frame Relay, qui utilisent différents systèmes d'adressage de couche 2. Quel que soit le type d'adressage de couche 2 utilisé, les trames sont conçues pour circuler dans un domaine de broadcast de

couche 2. Lorsque les données sont envoyées vers une unité de couche 3, les informations de couche 2 sont modifiées.

Lorsqu'une interface du routeur reçoit une trame, elle en extrait l'adresse MAC de destination. Cette adresse est vérifiée afin de savoir si la trame est destinée directement à l'interface du routeur ou s'il s'agit d'un broadcast. Dans les deux cas, la trame est acceptée. Si elle est destinée à une autre unité du domaine de collision, elle est rejetée.

Lorsqu'elle est acceptée, les informations de code de redondance cyclique (CRC, *Cyclic Redundancy Check*) sont extraites de son en-queue. Le CRC est calculé pour vérifier l'intégrité des données de la trame.

Si la vérification échoue, la trame est rejetée. Si elle réussit, l'en-queue et l'en-tête de trame sont retirés, et le paquet est transmis à la couche 3. Ce paquet est ensuite examiné pour savoir s'il est destiné au routeur ou s'il doit être acheminé vers un autre équipement de l'interréseau. Si l'adresse IP de destination correspond à l'un des ports du routeur, l'en-tête de la couche 3 est retiré et les données sont transmises à la couche 4. Dans le cas contraire, l'adresse est comparée à la table de routage. Si une correspondance est établie ou s'il existe un chemin par défaut, le paquet est envoyé à l'interface indiquée dans l'entrée mise en correspondance de la table de routage. Lors de la commutation du paquet vers l'interface de sortie, une nouvelle valeur CRC est ajoutée en en-queue de trame et l'en-tête de trame approprié est ajouté au paquet. La trame est ensuite transmise au domaine de broadcast suivant et continue sa route jusqu'à la destination finale.

La page suivante décrit deux types de services de transmission.

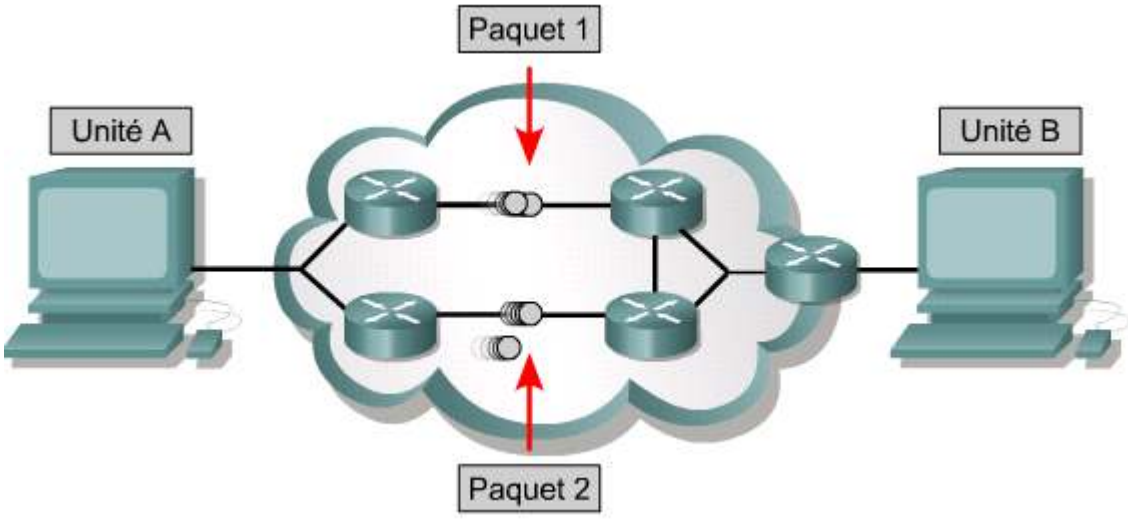
10.1 Protocole routé

10.1.4 Transmission orientée connexion et transmission non orientée connexion

Cette page présente deux types de systèmes de transmission, l'un orienté connexion et l'autre sans connexion.

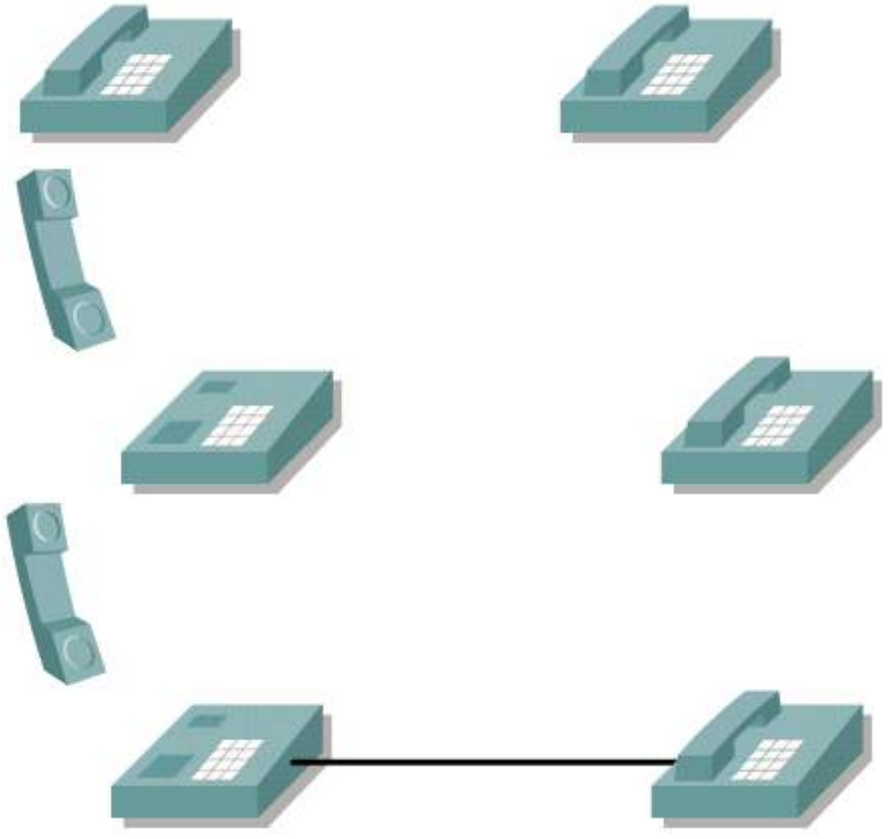
Ces deux services constituent la véritable transmission des données de bout en bout sur un interréseau.

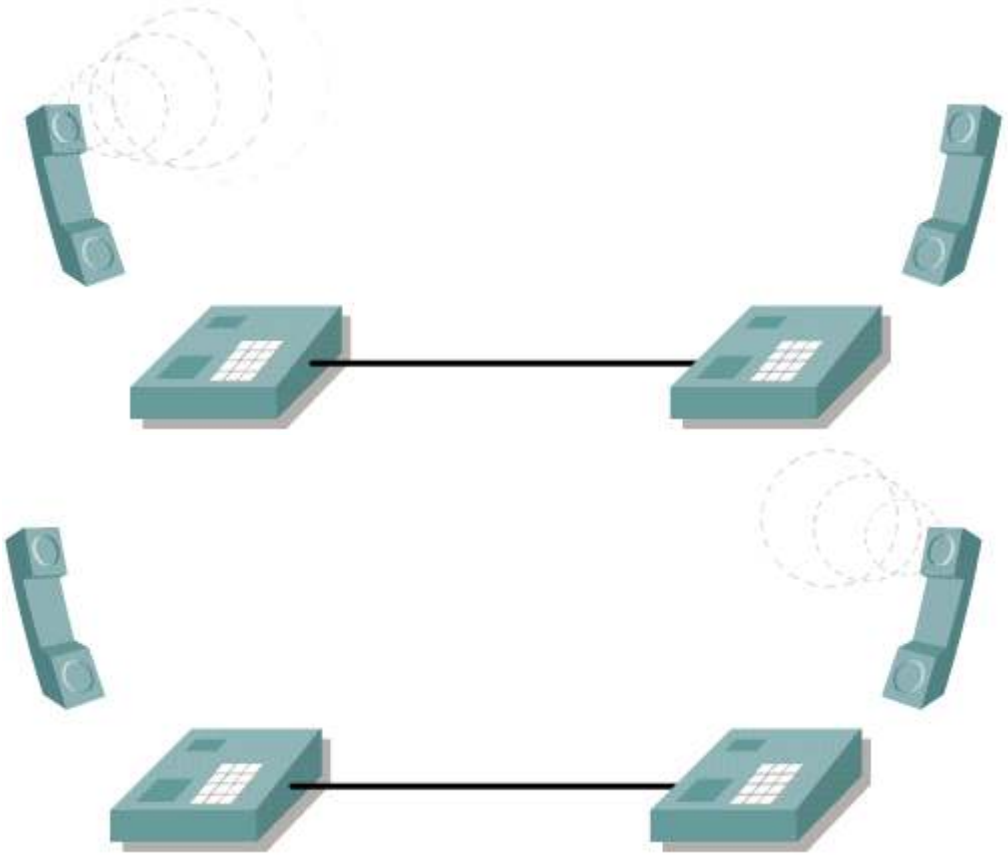
La plupart des services réseau utilisent un système de livraison non orienté connexion. 1



Les paquets peuvent emprunter différentes routes pour circuler sur le réseau. Ils sont ensuite rassemblés à leur arrivée. Dans un système non orienté connexion, la destination n'est pas contactée avant l'envoi d'un paquet. Le système postal constitue une bonne analogie, puisque le destinataire du courrier n'est pas contacté pour savoir s'il acceptera la lettre avant son envoi. De même, l'expéditeur ne sait pas si sa lettre est arrivée à bon port.

Dans les systèmes orientés connexion, une connexion est établie entre l'émetteur et le récepteur avant le transfert des données. 2





Le système téléphonique est un exemple de système orienté connexion. L'appelant initie l'appel, une connexion s'établit, puis la communication a lieu.

Les processus réseau sans connexion sont souvent appelés processus à commutation de paquets. Au cours de leur acheminement, les paquets peuvent emprunter différents chemins et arriver de manière désordonnée. Chaque paquet contient des informations, telles que l'adresse de destination ainsi que la position dans le message, ce qui permet de coordonner l'arrivée avec les autres paquets associés. Lorsque la destination est atteinte, les paquets sont ainsi réassemblés selon la bonne séquence. Le chemin emprunté par chaque paquet est déterminé par divers critères. Certains de ces critères, tels que la bande passante disponible, peuvent varier d'un paquet à l'autre.

Les processus réseau orientés connexion sont souvent appelés processus à commutation de circuits. Une connexion avec le destinataire est établie avant que le transfert des données ne commence. Tous les paquets circulent de manière séquentielle sur le même circuit virtuel ou physique.

Internet est un réseau sans connexion gigantesque, dans lequel la majorité des transmissions de paquets sont traitées par le protocole IP. Le protocole TCP ajoute les services orientés connexion et fiables de la couche 4 au protocole IP.

La page suivante donne des informations sur l'en-tête IP.

Les paquets IP comprennent les données des couches supérieures et un en-tête IP. Cette page présente le contenu de cet en-tête: [1]

0 4 8		16 19	24 31
VERS	HLEN	Type de service	Longueur totale
Identification		Indicateurs	Décalage de fragment
Durée de vie		Protocole	Somme de contrôle d'en-tête
Adresse IP source			
Adresse IP de destination			
Options IP (s'il y a lieu)			Remplissage
Données			
. . .			

Il s'agit des champs d'un en-tête de paquet IP. Leur longueur est fixe, sauf dans le cas des options IP et des champs de remplissage.

- **Version:** indique le format de l'en-tête du paquet IP. Le champ Version (4 bits) contient le numéro 4 s'il s'agit d'un paquet IPv4 ou le numéro 6 s'il s'agit d'un paquet IPv6. Ce champ n'est toutefois pas utilisé pour faire la distinction entre des paquets IPv4 et IPv6. C'est le rôle du champ relatif au type de protocole présent dans l'enveloppe de couche 2.
- **Longueur d'en-tête IP (HLEN):** indique la longueur de l'en-tête du datagramme en mots de 32 bits. Ce champ représente la longueur totale des informations d'en-tête et inclut les deux champs d'en-tête de longueur variable.
- **Type de service (ToS):** ce champ codé sur 8 bits indique le niveau d'importance attribué par un protocole de couche supérieure particulier.
- **Longueur totale (16 bits):** ce champ spécifie la taille totale du paquet en octets, données et en-tête inclus. Pour obtenir la taille des données proprement dites, soustrayez la longueur de l'en-tête IP de cette longueur totale.
- **Identification (16 bits):** identifie le datagramme actuel. Ce champ comporte le numéro de séquence.
- **Drapeaux (3 bits):** champ dans lequel les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment d'une série de paquets fragmentés.
- **Décalage de fragment (13 bits):** champ permettant de rassembler les fragments du datagramme. Il permet au champ précédent de se terminer sur une frontière de 16 bits.
- **Durée de vie (TTL):** champ indiquant le nombre de sauts par lesquels un paquet peut passer. Ce nombre est décrémenté à chaque passage du paquet dans un routeur. Lorsque le compteur atteint zéro, le paquet est éliminé. Cela empêche les paquets de circuler indéfiniment en boucle.
- **Protocole (8 bits):** indique quel protocole de couche supérieure, tel que TCP ou UDP, reçoit les paquets entrants une fois les processus IP terminés.
- **Somme de contrôle de l'en-tête (16 bits):** champ qui aide à garantir l'intégrité de l'en-tête IP.
- **Adresse source (32 bits):** : champ indiquant l'adresse IP du nœud à partir duquel a été envoyé le paquet.
- **Adresse de destination (32 bits):** champ indiquant l'adresse IP du nœud vers lequel sont envoyées les données.
- **Options:** permet au protocole IP de prendre en charge diverses options, telles que la sécurité. La longueur de ce champ peut varier.

- **Remplissage:** des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.
- **Données:** ce champ contient les informations de couche supérieure. Sa longueur est variable.

Si les adresses IP source et de destination sont des champs capitaux, les autres champs de l'en-tête font du protocole IP un protocole très souple. Les champs de l'en-tête répertorient les informations d'adressage source et de destination du paquet et indiquent souvent la longueur des données du message. Les informations de routage sont également contenues dans les en-têtes IP, qui, de ce fait, peuvent devenir longs et complexes.

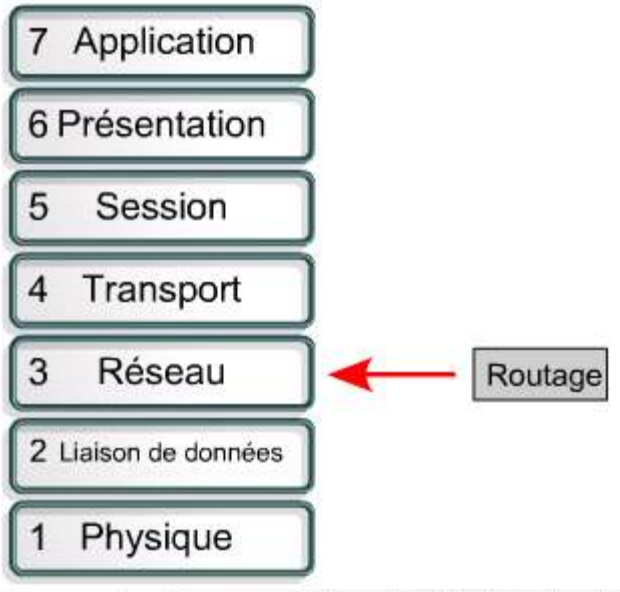
Cette page termine la leçon. La leçon suivante porte sur les protocoles de routage IP. La première page donne une vue d'ensemble du routage.

10.2 Protocoles de routage IP

10.2.1 Vue d'ensemble du routage

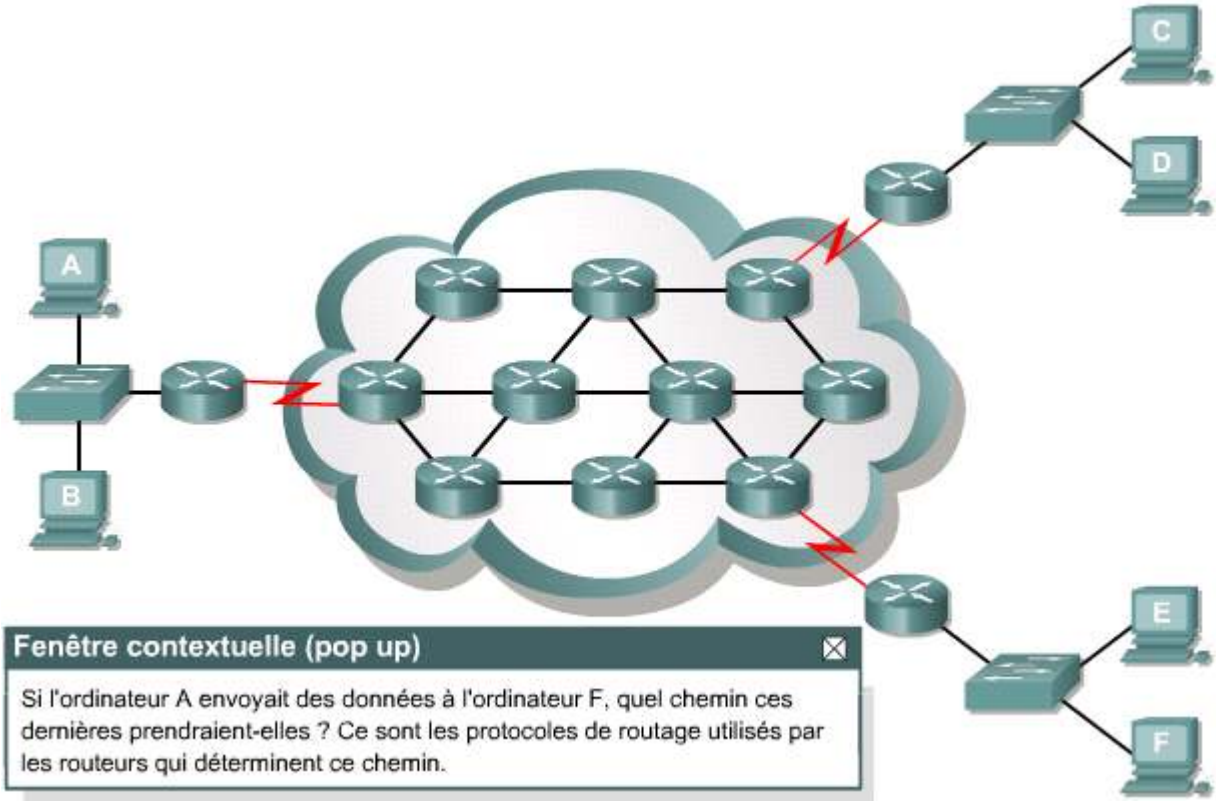
Cette page aborde le routage et présente les deux principales fonctions du routeur.

Le routage est une fonction de la couche 3 du modèle OSI. 1



La couche réseau est chargée d'acheminer les paquets sur un réseau.

C'est un système d'organisation hiérarchique qui permet de regrouper des adresses individuelles. Ces dernières sont traitées comme un tout jusqu'à ce que l'adresse de destination soit requise pour la livraison finale des données. (Vu prècedement)2

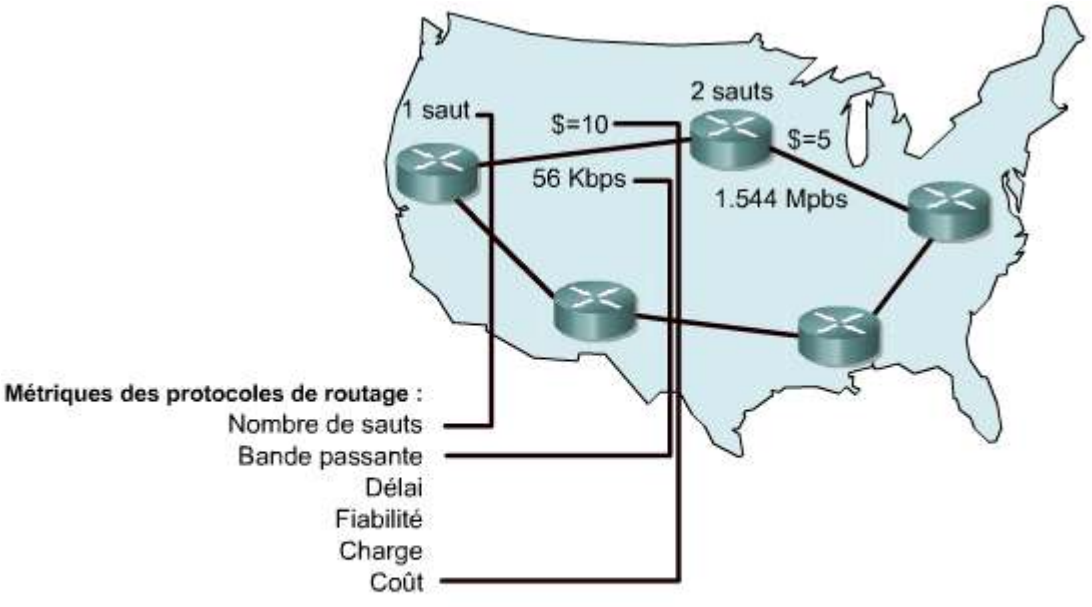

A
B
C
D
E
F
Fenêtre contextuelle (pop up)
Si l'ordinateur A envoyait des données à l'ordinateur F, quel chemin ces dernières prendraient-elles ? Ce sont les protocoles de routage utilisés par les routeurs qui déterminent ce chemin.

Le routage cherche le chemin le plus efficace d'une unité à une autre. Le matériel au centre du processus de routage est le routeur.

Il possède les deux fonctions principales suivantes:

- Le routeur gère les tables de routage et s'assure que les autres routeurs ont connaissance des modifications apportées à la topologie du réseau. Il se sert des protocoles de routage pour échanger les informations de réseau.
- Le routeur détermine la destination des paquets à l'aide de la table de routage lorsque ceux-ci arrivent à l'une de ses interfaces. Il les transfère vers la bonne interface, ajoute les informations de trame de cette interface, puis transmet la trame.

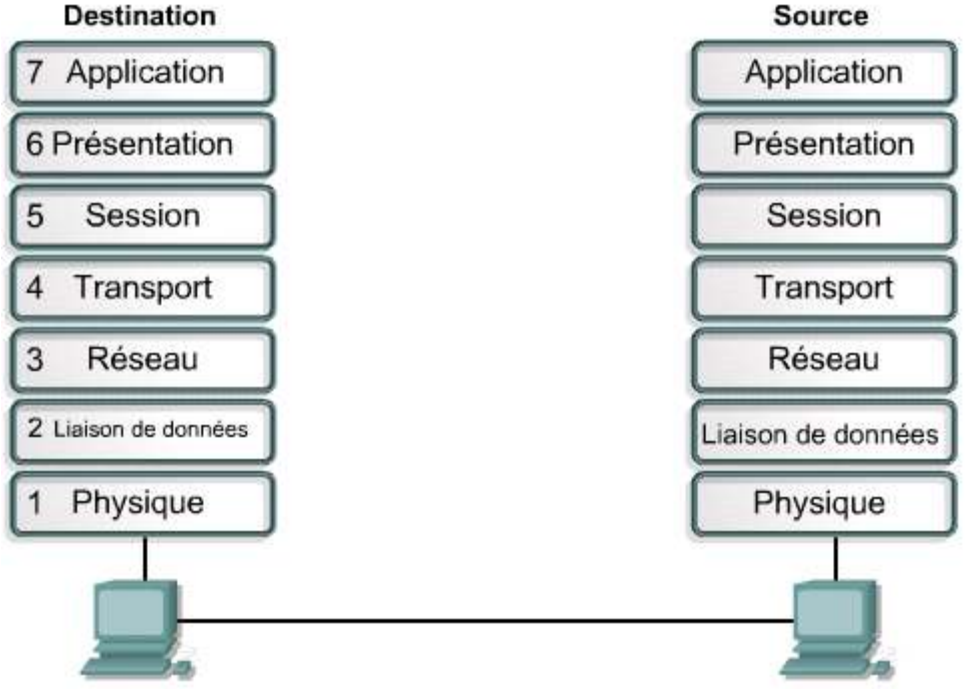
Un routeur est une unité de couche réseau qui utilise une ou plusieurs métriques pour déterminer le chemin optimal par lequel acheminer le trafic réseau. Les métriques de routage sont les valeurs qui permettent de définir le meilleur chemin. 3

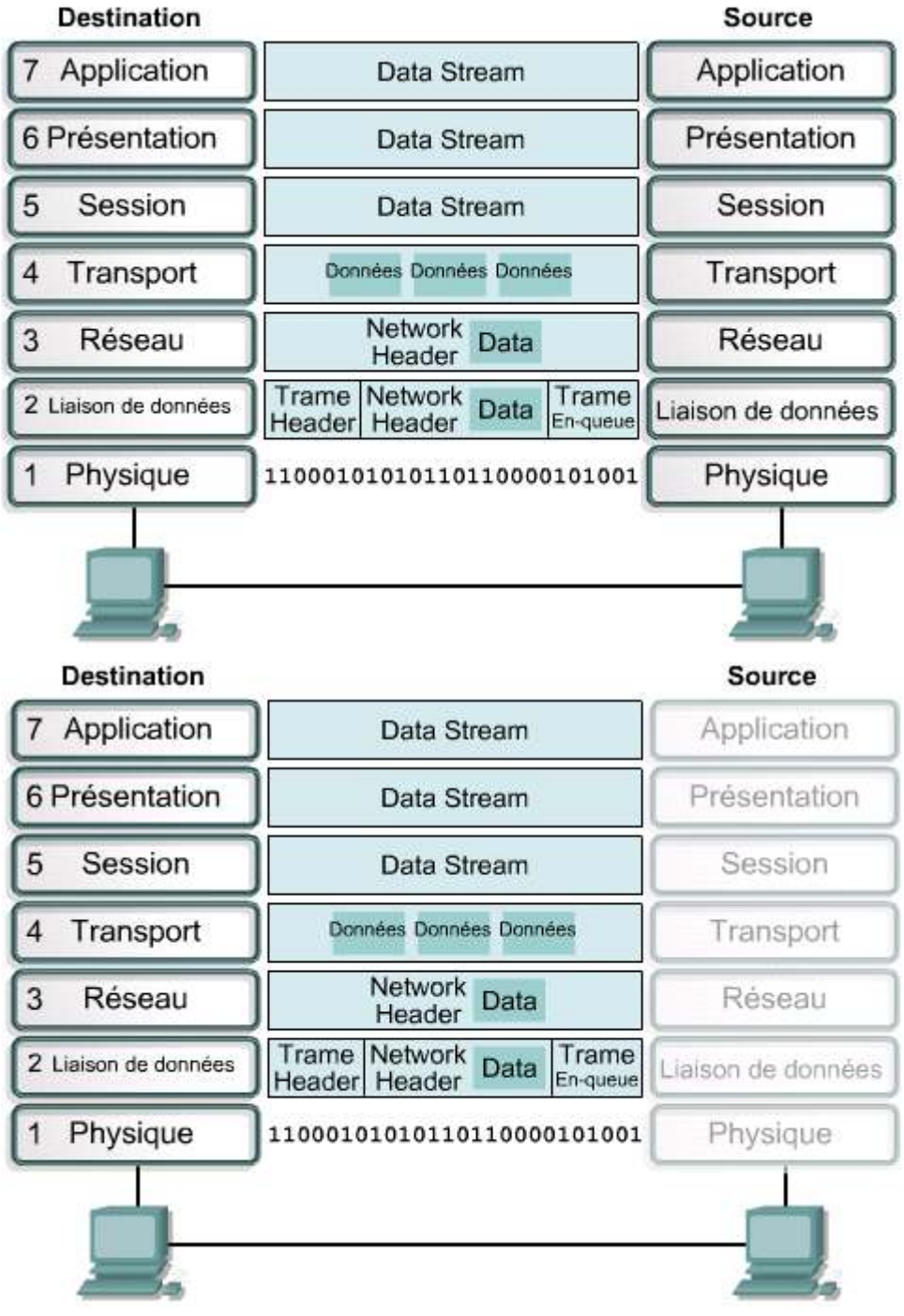


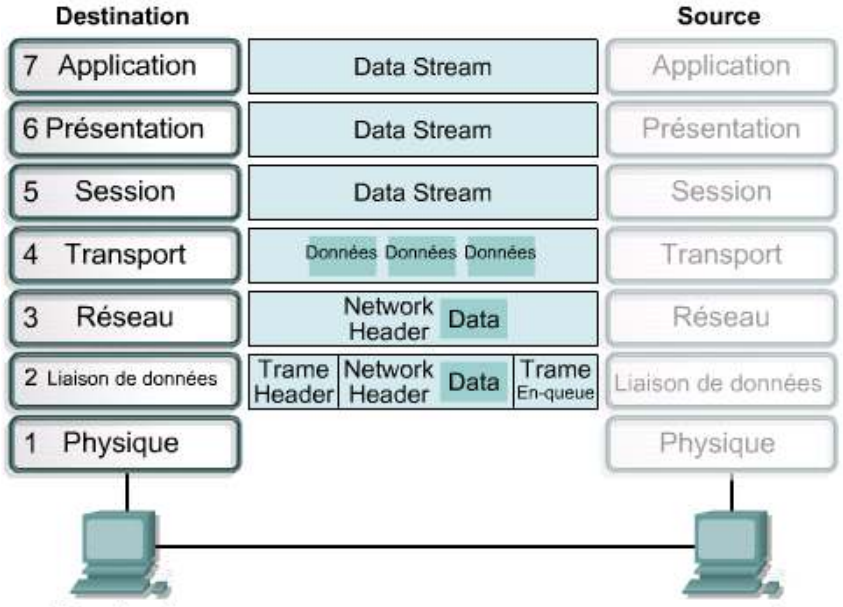
La couche réseau est chargée d'acheminer les paquets sur un réseau.

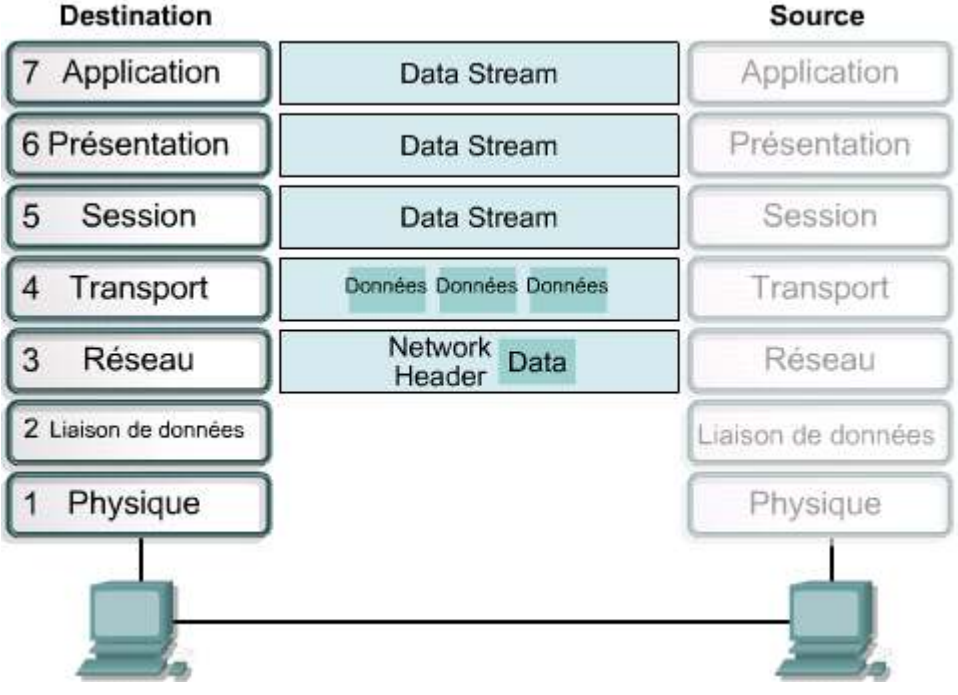
Les protocoles de routage utilisent diverses combinaisons de ces métriques pour établir la meilleure route possible des données.

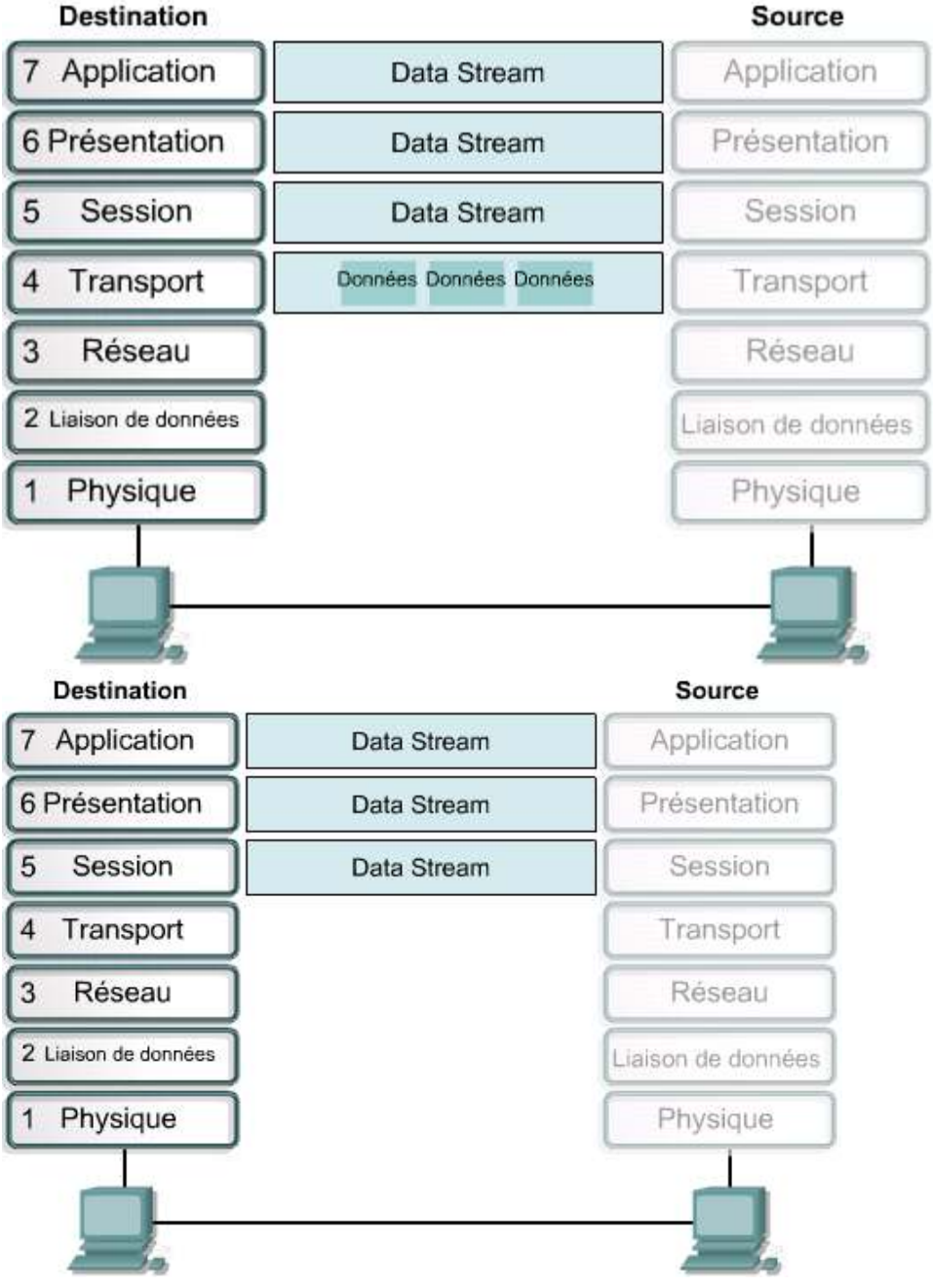
Les routeurs permettent d'interconnecter les segments d'un réseau ou des réseaux entiers. Leur rôle consiste à acheminer les trames de données entre les réseaux, en fonction des informations de la couche 3. Ils prennent des décisions logiques quant au meilleur acheminement possible des données, puis redirigent les paquets vers le port de sortie approprié afin qu'ils soient encapsulés pour la transmission. 4

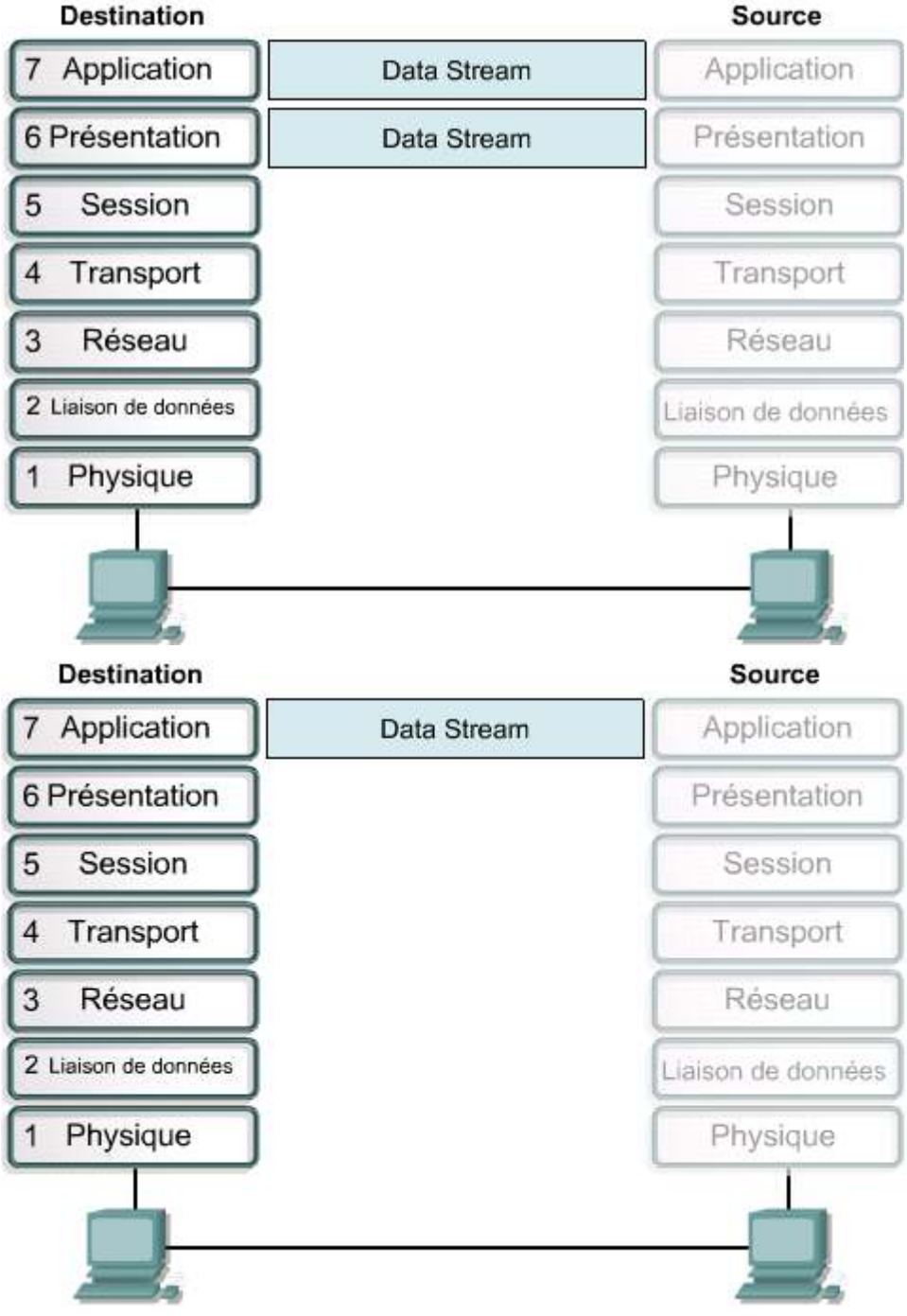


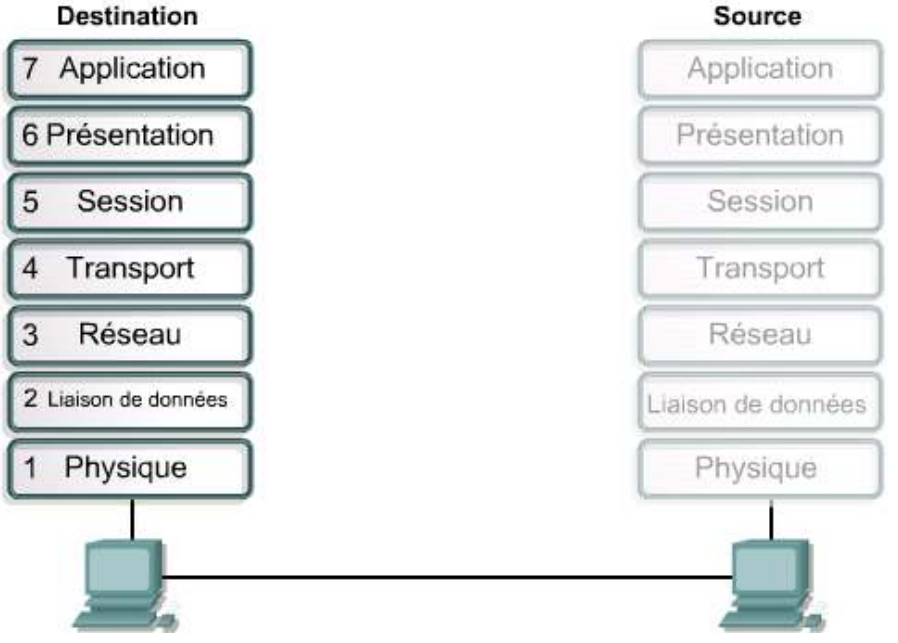

Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Données Données Données
Transport
3 Réseau
Network Header
Data
Réseau
2 Liaison de données
Trame Header
Network Header
Data
Trame En-queue
Liaison de données
1 Physique
1100010101011011000010100 1
Physique
Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Données Données Données
Transport
3 Réseau
Network Header
Data
Réseau
2 Liaison de données
Trame Header
Network Header
Data
Trame En-queue
Liaison de données
1 Physique
1100010101011011000010100 1
Physique


Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Données Données Données
Transport
3 Réseau
Network Header
Data
Réseau
2 Liaison de données
Trame Header
Network Header
Data
Trame En-queue
Liaison de données
1 Physique
Physique


Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Données Données Données
Transport
3 Réseau
Network Header
Data
Réseau
2 Liaison de données
Liaison de données
1 Physique
Physique


Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Données Données Données
Transport
3 Réseau
Réseau
2 Liaison de données
Liaison de données
1 Physique
Physique
Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Data Stream
Session
4 Transport
Transport
3 Réseau
Réseau
2 Liaison de données
Liaison de données
1 Physique
Physique


Destination
Source
7 Application
Data Stream
Application
6 Présentation
Data Stream
Présentation
5 Session
Session
4 Transport
Transport
3 Réseau
Réseau
2 Liaison de données
Liaison de données
1 Physique
Physique
Destination
Source
7 Application
Data Stream
Application
6 Présentation
Présentation
5 Session
Session
4 Transport
Transport
3 Réseau
Réseau
2 Liaison de données
Liaison de données
1 Physique
Physique

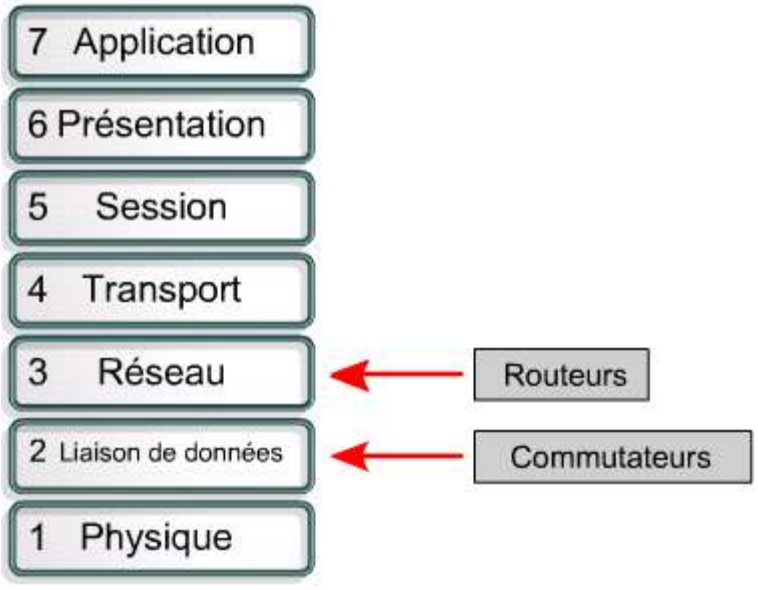


Les phases d'encapsulation et de désencapsulation se produisent à chaque passage d'un paquet dans un routeur. Le routeur doit en effet désencapsuler la trame de données de la couche 2 pour accéder à l'adresse de couche 3 et l'examiner. Comme vous pouvez le voir dans la figure 5, le processus intégral d'envoi des données implique des phases d'encapsulation et de désencapsulation au niveau des sept couches du modèle OSI. L'encapsulation consiste à fractionner le flux de données en segments et à ajouter les en-têtes et les en-queues appropriés avant de transmettre les données. Le processus de désencapsulation, quant à lui, consiste à retirer les en-têtes et les en-queues, puis à recombiner les données en un flux continu.

Ce cours présente le protocole routable le plus répandu, à savoir IP. D'autres protocoles routables existent, comme par exemple IPX/SPX et AppleTalk. Ces protocoles prennent en charge la couche 3. Ceux qui ne la prennent pas en charge sont des protocoles non routables. Le plus connu d'entre eux est NetBEUI. Il s'agit d'un petit protocole rapide et efficace qui se contente de livrer les trames sur un seul segment.

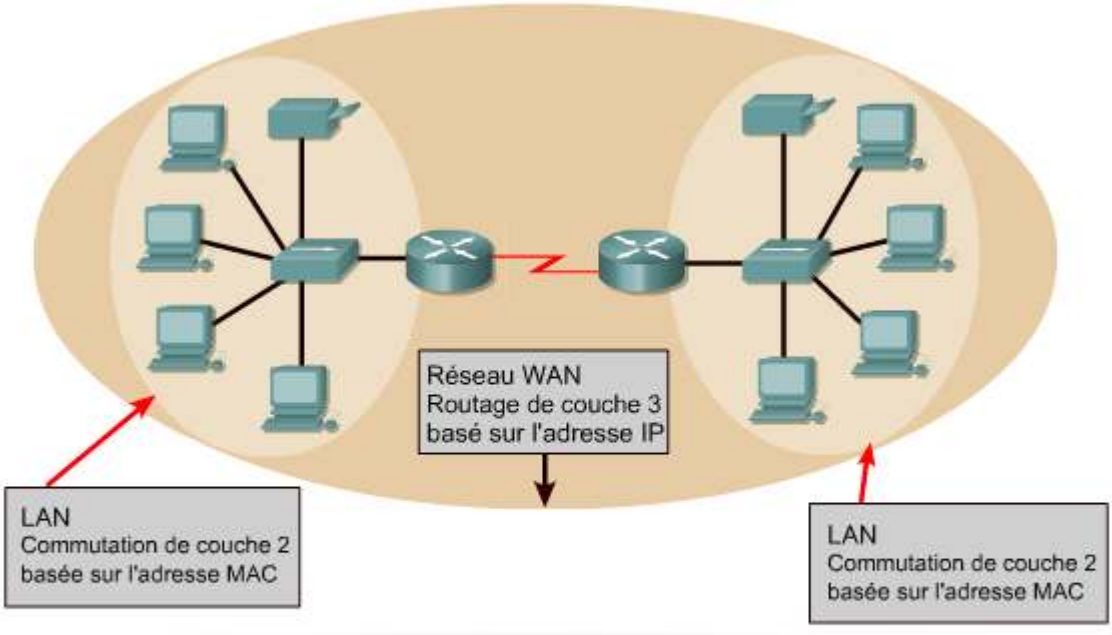
La page suivante explique les différences existant entre le routage et la commutation.

Cette page effectue une comparaison entre le routage et la commutation. 1



En apparence, les routeurs et les commutateurs semblent jouer le même rôle. La principale différence entre les deux repose sur le fait que les commutateurs opèrent au niveau de la couche 2 du modèle OSI alors que les routeurs fonctionnent sur la couche 3. Autrement dit, ces deux matériels utilisent des informations différentes pour envoyer les données de la source à la destination.

La relation existant entre la commutation et le routage peut être comparée aux appels téléphoniques locaux et longue distance. Lorsqu'un appel est passé à un numéro comportant le même indicatif régional, il est traité par un commutateur local. Ce dernier ne peut effectuer le suivi que des numéros locaux. Il ne peut pas gérer l'ensemble des numéros de téléphone du monde entier. Lorsque le commutateur reçoit une demande pour un appel hors de sa zone, il transfère cet appel vers un commutateur de niveau supérieur à même de reconnaître les indicatifs régionaux. Celui-ci commute ensuite l'appel de sorte qu'il atteigne le commutateur local correspondant à son indicatif. 2



La commutation de couche 2 s'effectue au sein du réseau LAN. Le routage de couche 3 achemine le trafic entre les domaines de broadcast. Cela nécessite le format d'adressage hiérarchique d'un système d'adressage de couche 3, tel que IP.

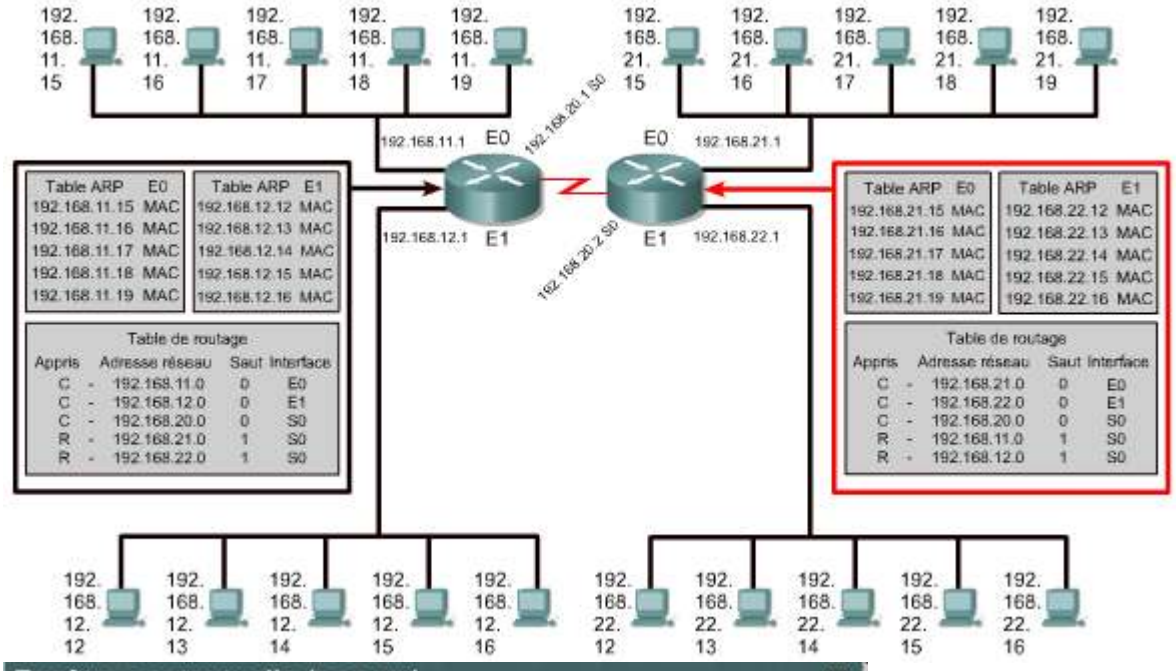
Le routeur joue un rôle similaire à celui du commutateur de niveau supérieur. La figure 3

montre les tables ARP des adresses MAC de la couche 2 et les tables de routage des adresses IP de la couche 3. Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque entrée de table ARP contient une paire d'adresses IP-MAC.

Le commutateur de couche 2 établit sa table de transmission à l'aide d'adresses MAC. Lorsqu'un hôte possède des données pour une adresse IP non locale, il envoie la trame au routeur le plus proche. Ce routeur est également appelé « passerelle par défaut ». L'hôte se sert de l'adresse MAC du routeur comme adresse MAC de destination.

Un commutateur interconnecte des segments appartenant au même réseau ou sous-réseau logique. 2 Dans le cas d'hôtes non locaux, le commutateur transfère la trame au routeur en fonction de l'adresse MAC de destination. Le routeur analyse alors l'adresse de destination de couche 3 du paquet afin de déterminer l'acheminement de la trame. L'hôte X connaît l'adresse IP du routeur parce que sa configuration IP contient l'adresse IP de la passerelle par défaut.

À l'instar du commutateur qui gère une table d'adresses MAC connues, le routeur possède une table d'adresses IP connue sous le nom de table de routage. 3



Fenêtre contextuelle (pop up)

Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque table ARP contient une paire d'adresses IP-MAC. Les adresses MAC sont représentées dans le schéma avec l'acronyme MAC, les adresses réelles étant trop longues pour pouvoir figurer ici. Les tables de routage cherchent également à savoir comment la route a été apprise. Dans cet exemple, elles sont directement connectées (représentées par un C) ou apprises par le biais du protocole RIP (représentées par un R). Les tables permettent de déterminer l'adresse IP des réseaux à atteindre, le nombre de sauts ou la distance jusqu'à ces réseaux, ainsi que l'interface à partir de laquelle les données doivent être acheminées pour atteindre le réseau de destination.

Les adresses MAC ne sont pas organisées de manière logique, tandis que l'organisation des adresses IP est, elle, hiérarchique. Un commutateur se contentant de rechercher les adresses appartenant à son segment dans sa table, il ne traite qu'un nombre limité d'adresses MAC non organisées. Les routeurs, quant à eux, ont besoin d'un système d'adressage hiérarchique qui va permettre de regrouper les adresses similaires et de les traiter en tant qu'une seule et même unité réseau, et ce jusqu'à ce que les données atteignent le segment de destination.

Sans cette organisation, Internet ne pourrait fonctionner. Vous pourriez comparer ce dernier à une bibliothèque dans laquelle des millions de pages imprimées s'entasseraient. Cette documentation serait tout simplement inutile puisqu'il serait impossible de localiser un seul de ces documents. Lorsque ces pages sont identifiées et assemblées en un livre et que chacun de ces livres est répertorié dans un index, la recherche et l'utilisation des données deviennent alors possibles.

Une autre différence entre les réseaux routés et commutés réside dans le fait que ces derniers ne bloquent pas les broadcasts. 4

Fonctions	Routeur	Commutateur
Vitesse	Lente	Rapide
Couches OSI	Couche 3	Couche 2
Adressage utilisé	IP	MAC
Broadcasts	Bloqués	Transmis
Sécurité	Élevée	Faible

La vitesse et la sécurité sont relatives et dépendent de la configuration de l'équipement.

Les commutateurs peuvent par conséquent voir leur fonctionnement perturbé par des tempêtes de broadcasts. Les routeurs bloquant les broadcasts LAN, les tempêtes n'affectent que le domaine de broadcast dont elles sont issues. Du fait de ce blocage, les routeurs offrent une meilleure sécurité et un meilleur contrôle de la bande passante que les commutateurs.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux appréhender les différences existant entre le routage et la commutation.

La page suivante compare les protocoles de routage et les protocoles routés.

Activité de média interactive

Glisser-Positionner: Routage et commutation

À l'issue de cette activité, les étudiants seront capables de faire la distinction entre le routage et la commutation.

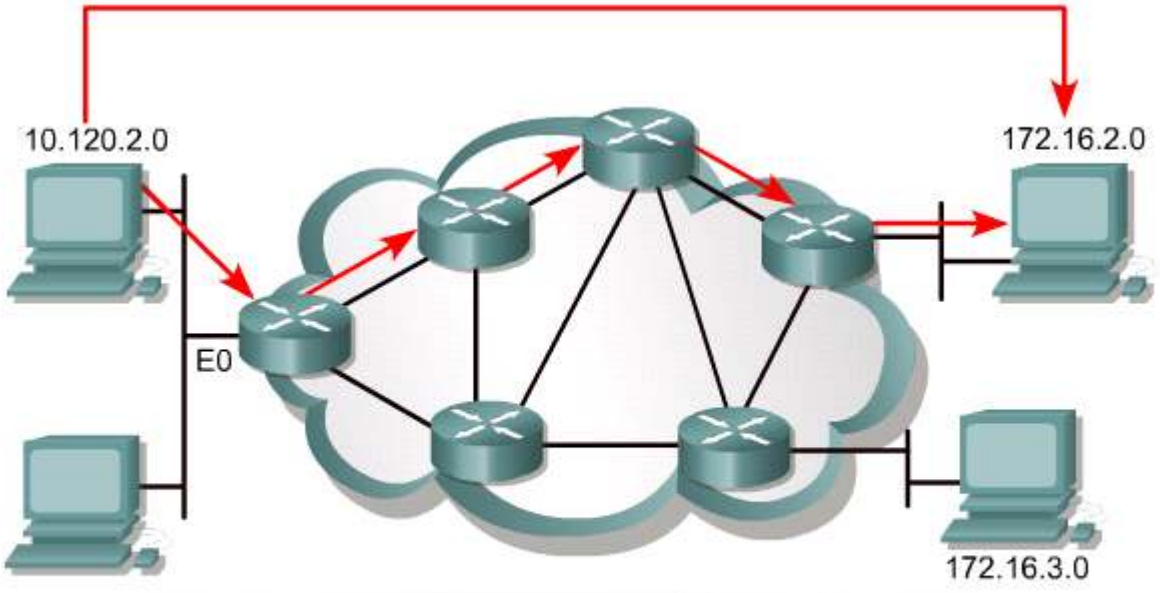
10.2 Protocoles de routage IP

10.2.3 Protocole routé et protocole de routage

Cette page explique les différences entre un protocole de routage et un protocole routé.

Les protocoles routés ou routables sont utilisés au niveau de la couche réseau afin de transférer les données d'un hôte à l'autre via un routeur. Les protocoles routés transportent les données sur un réseau. Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin possible pour acheminer les données de la source vers leur destination.

Le protocole routé englobe notamment les fonctions suivantes: 1



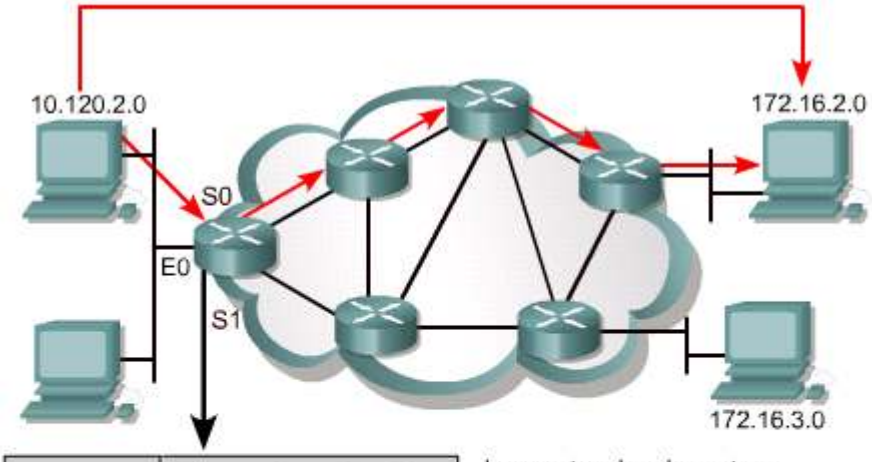
Les protocoles routés transportent les données d'une station d'extrémité à une autre.

- Il inclut n'importe quelle suite de protocoles réseau capable de fournir assez d'informations dans l'adresse de couche réseau pour permettre au routeur d'effectuer le transfert vers l'unité suivante, jusqu'à la destination finale.
- Il définit le format et l'usage des champs dans un paquet.

Le protocole IP (*Internet Protocol*) et le protocole IPX (*Internetwork Packet Exchange*) de Novell, mais aussi DECnet, AppleTalk, Banyan VINES et Xerox Network Systems (XNS), sont des exemples de protocoles routés.

Les routeurs utilisent des protocoles de routage pour échanger des tables de routage et partager d'autres informations d'acheminement. En d'autres termes, les protocoles de routage permettent aux routeurs d'acheminer les protocoles routés.

Les fonctions du protocole de routage sont en partie les suivantes: 2



Protocole réseau	Réseau de destination	Interface de sortie
Connecté	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Protocole de routage = RIP, IGRP

Les protocoles de routage sont utilisés par les routeurs pour déterminer les chemins et gérer les tables de routage.
Une fois le chemin déterminé, le routeur peut acheminer le protocole routé.

- Il fournit les processus utilisés pour partager les informations d'acheminement.
- Il permet aux routeurs de communiquer entre eux afin de mettre à jour et de gérer les tables de routage.

Les protocoles de routage prenant en charge le protocole routé IP sont par exemple les protocoles RIP, IGRP, OSPF, BGP et EIGRP.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux appréhender les différences existant entre les protocoles routés et les protocoles de routage.

La page suivante aborde la manière dont le chemin des paquets est déterminé.

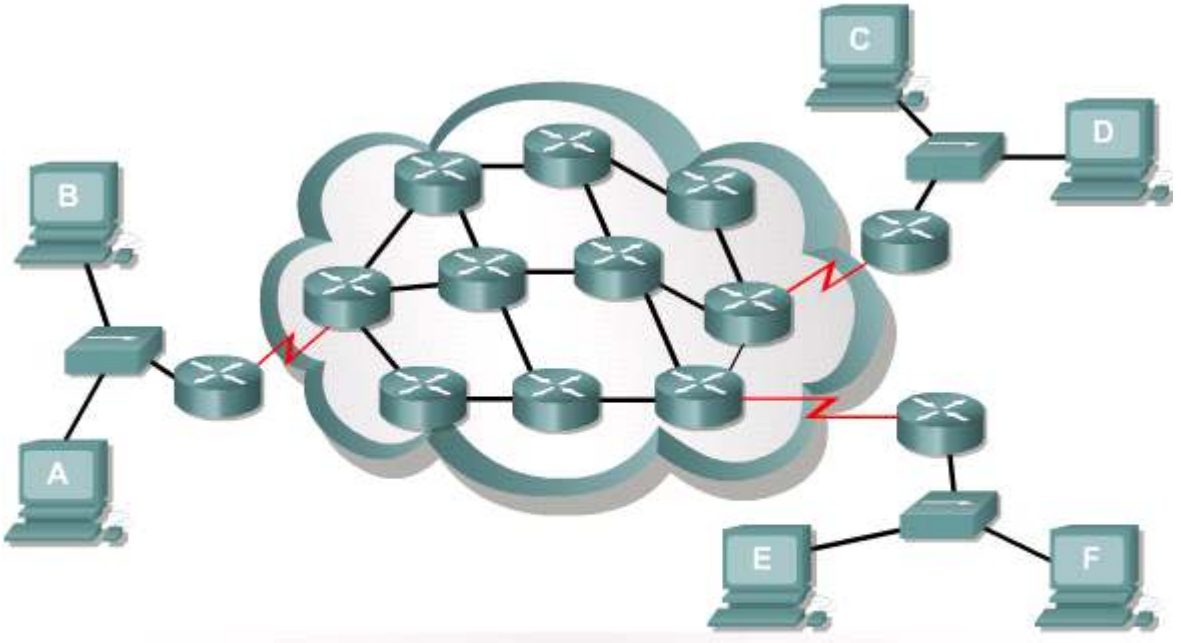
Activité de média interactive

Case à cocher: Protocole routé et protocole de routage

À l'issue de cette activité, les étudiants seront capables de faire la distinction entre les protocoles de routage et les protocoles routés.

Cette page explique le mécanisme de la sélection du chemin.

La détermination du chemin se produit au niveau de la couche réseau. 1

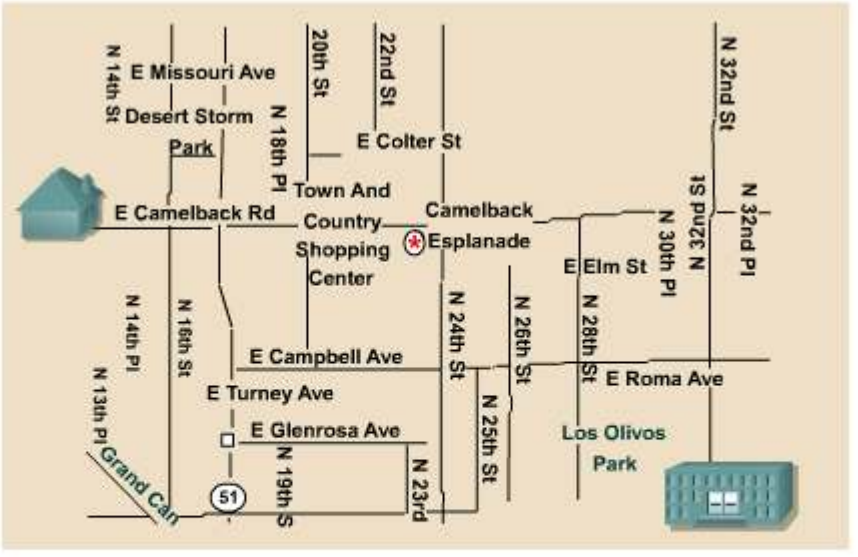


Si l'ordinateur A envoyait des données à l'ordinateur F, quel chemin ces dernières prendraient-elles ? Ce chemin est déterminé par les informations contenues dans la table de routage.

Ce processus permet au routeur de comparer l'adresse de destination aux routes disponibles dans sa table de routage et de choisir le meilleur chemin possible. Les routeurs acquièrent ces chemins soit par l'intermédiaire du routage statique, soit par l'intermédiaire du routage dynamique. Les chemins configurés manuellement par l'administrateur réseau sont appelés «routes statiques». Ceux que le routeur a acquis d'autres routeurs à l'aide d'un protocole de routage sont dits «routes dynamiques».

La détermination du chemin permet au routeur de choisir le port à partir duquel envoyer un paquet pour que celui-ci arrive à destination.

2

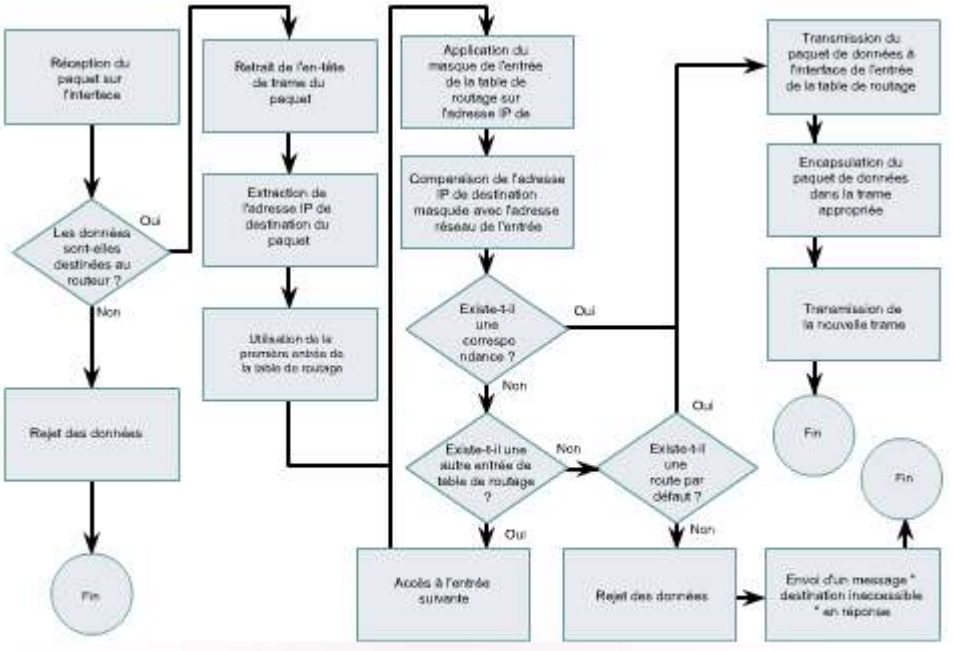


Quel est le meilleur chemin de votre maison à l'université ? Plusieurs routes existent, mais vous vous demanderez quelle est la plus courte, la plus rapide, la plus sûre et la plus fiable. Lors de l'acheminement des données, ce sont ces mêmes questions qui sont posées et résolues.

On appelle ce processus le routage d'un paquet. Chaque routeur rencontré sur le chemin du paquet est appelé un saut. Le nombre de sauts constitue la distance parcourue. La détermination du chemin peut être comparée à la situation où une personne conduit sa voiture d'un endroit de la ville à un autre. Le conducteur consulte une carte qui lui indique les rues par lesquelles passer pour arriver à sa destination, tout comme le routeur consulte sa table de routage. Il passe d'un carrefour à un autre, de la même façon qu'un paquet circule d'un routeur à un autre lors de chaque saut. À chaque carrefour, le conducteur peut choisir de prendre à gauche, à droite ou de continuer tout droit. Il en va de même pour le routeur lorsqu'il choisit le port de sortie à partir duquel le paquet sera envoyé.

Le conducteur prend ses décisions en fonction de certains facteurs, comme l'état du trafic, la limitation de vitesse, le nombre de voies, les péages et si une route est fréquemment fermée ou pas. Il est parfois plus rapide de prendre le chemin le plus long en passant par des petites routes peu fréquentées que de prendre l'autoroute embouteillée. De même, les routeurs vont prendre leurs décisions en fonction de la charge, de la bande passante, du délai, du coût et de la fiabilité d'une liaison de réseau.

Les processus impliqués dans la sélection du chemin pour chaque paquet sont les suivants: 3


Réception du paquet sur l'interface
Les données sont-elles destinées au routeur ?
Oui
Non
Rejet des données
Fin
Retrait de l'en-tête de trame du paquet
Extraction de l'adresse IP de destination du paquet
Utilisation de la première entrée de la table de routage
Application du masque de l'entrée de la table de routage sur l'adresse IP de
Comparaison de l'adresse IP de destination masquée avec l'adresse réseau de l'entrée
Existe-t-il une correspondance ?
Oui
Non
Existe-t-il une autre entrée de table de routage ?
Non
Oui
Accès à l'entrée suivante
Existe-t-il une route par défaut ?
Oui
Non
Rejet des données
Transmission du paquet de données à l'interface de l'entrée de la table de routage
Encapsulation du paquet de données dans la trame appropriée
Transmission de la nouvelle trame
Fin
Envoi d'un message " destination inaccessible " en réponse
Fin

Il s'agit là du processus fondamental de l'acheminement des données par un routeur, même si certaines étapes n'ont pas été mentionnées ici pour des soucis de clarté.

- Le routeur compare l'adresse IP du paquet reçu avec ses tables IP.
- Il extrait l'adresse de destination du paquet.
- Le masque de la première entrée dans la table de routage est appliqué à l'adresse de destination.
- La destination masquée est comparée avec l'entrée de la table de routage.
- Si une correspondance est établie, le paquet est transmis au port associé à cette entrée de table.
- Si aucune correspondance n'est établie, l'entrée suivante de la table est examinée.
- Si le paquet ne correspond à aucune des entrées de la table, le routeur recherche l'existence d'une route par défaut.
- Si une route par défaut a été définie, le paquet est transmis au port qui lui est associé. La route par défaut est le chemin qui doit être utilisé lorsque aucune correspondance n'a pu être établie avec la table de routage. Elle est configurée par l'administrateur réseau.
- Si aucun chemin par défaut n'existe, le paquet est éliminé. Un message est alors souvent envoyé à l'unité émettrice des données pour signaler que la destination n'a pu être atteinte.

Les étudiants peuvent effectuer l'activité de média interactive pour mieux cerner le processus de détermination du chemin.

La page suivante explique comment les protocoles de routage construisent et gèrent les tables de routage.

Activité de média interactive

Glisser-Positionner: Organigramme de la détermination du chemin

À l'issue de cette activité, les étudiants seront capables d'expliquer en détail le processus de détermination du chemin.

Cette page décrit le rôle d'une table de routage.

Les routeurs emploient des protocoles de routage pour construire et gérer les tables de routage contenant les informations d'acheminement. Le processus de sélection du chemin en est ainsi facilité. Les protocoles de routage placent diverses informations d'acheminement dans les tables de routage. Le contenu de ces informations varie selon le protocole de routage utilisé. Les tables de routage contiennent les informations nécessaires à la transmission des paquets de données sur les réseaux connectés. Les équipements de couche 3 interconnectent les domaines de broadcast ou les réseaux LAN. Le transfert des données nécessite un système d'adressage hiérarchique. 1

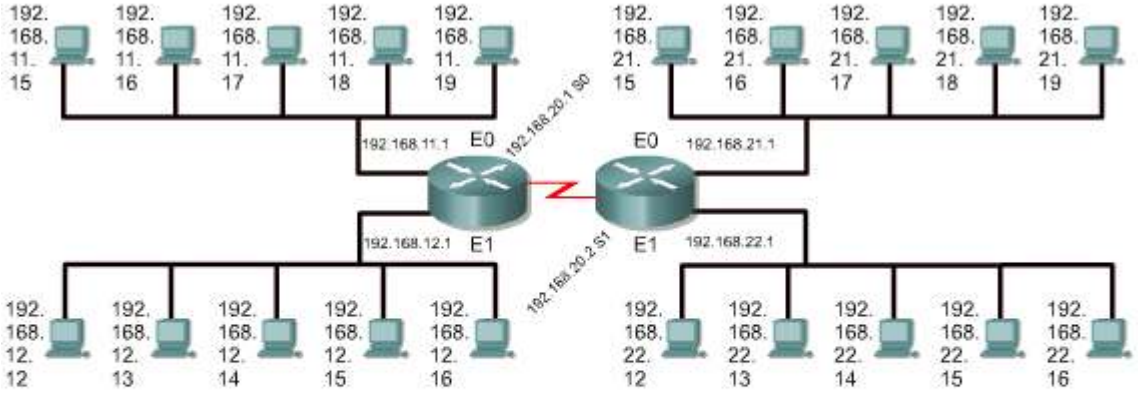


Table de routage

Appris	Adresse réseau	Saut	Interface
C -	192.168.11.0	0	E0
C -	192.168.12.0	0	E1
C -	192.168.20.0	0	S0
R -	192.168.21.0	1	S0
R -	192.168.22.0	1	S0

Table de routage

Appris	Adresse réseau	Saut	Interface
C -	192.168.21.0	0	E0
C -	192.168.22.0	0	E1
C -	192.168.20.0	0	S1
R -	192.168.11.0	1	S1
R -	192.168.12.0	1	S1

Les routeurs conservent les informations suivantes dans leurs tables de routage:

- **Type de protocole:** cette information identifie le type de protocole de routage qui a créé chaque entrée.
- **Associations du saut suivant:** indique au routeur que la destination lui est directement connectée, ou qu'elle peut être atteinte par le biais d'un autre routeur appelé le «saut suivant» vers la destination finale. Dès réception d'un paquet, le routeur vérifie l'adresse de destination et tente de trouver une correspondance dans sa table de routage.
- **Métrique de routage:** les métriques utilisées varient selon les protocoles de routage et permettent de déterminer les avantages d'une route sur une autre. Par exemple, le protocole RIP se sert d'une seule métrique de routage : le nombre de sauts. Le protocole IGRP crée une valeur de métrique composite à partir des métriques de fiabilité, de délai, de charge et de bande passante.
- **Interfaces de sortie:** cette information désigne l'interface à partir de laquelle les données doivent être envoyées pour atteindre leur destination finale.

Les routeurs s'envoient des messages afin de mettre à jour leurs tables de routage. Certains protocoles de routage transmettent ces messages de manière périodique. D'autres ne les envoient que lorsque des changements sont intervenus dans la topologie du réseau. Certains transmettent l'intégralité de la table dans leurs messages de mise à jour alors que d'autres se contentent d'envoyer les modifications. L'analyse des mises

à jour de routage provenant de routeurs directement connectés permet aux routeurs de créer et de gérer leur table de routage.

La page suivante explique les métriques et les algorithmes de routage.

10.2 Protocoles de routage IP

10.2.6 Algorithmes et métriques de routage

Cette page présente les algorithmes et les métriques associés aux routeurs.

Un algorithme est une solution détaillée d'un problème. Les algorithmes utilisés pour définir le port auquel envoyer un paquet diffèrent selon les protocoles de routage. Ils reposent sur l'utilisation de métriques pour prendre ce type de décision.

Les protocoles de routage sont conçus pour répondre à un ou plusieurs des objectifs suivants:

- **Optimisation:** capacité d'un algorithme de routage à sélectionner le meilleur chemin. Ce dernier sera choisi en fonction des métriques et de la pondération utilisées dans le calcul. Par exemple, un algorithme peut utiliser à la fois le nombre de sauts et le délai comme métriques, mais considérer que le délai doit prévaloir dans le calcul.
- **Simplicité et réduction du temps-système:** plus l'algorithme est simple et plus il sera traité efficacement par le processeur et la mémoire du routeur. Ce paramètre est important si le réseau veut pouvoir évoluer vers des proportions plus conséquentes, comme Internet.
- **Efficacité et stabilité:** un algorithme de routage doit pouvoir fonctionner correctement dans des circonstances inhabituelles ou imprévues, comme les défaillances de matériels, les surcharges et les erreurs de mise en œuvre.
- **Flexibilité:** : un algorithme de routage doit pouvoir s'adapter rapidement à toutes sortes de modifications du réseau, touchant par exemple la disponibilité et la mémoire du routeur, la bande passante ou le délai réseau.
- **Rapidité de convergence:** la convergence est le processus par lequel tous les routeurs s'entendent sur les routes disponibles. Lorsqu'un événement sur le réseau entraîne des modifications au niveau de la disponibilité d'un routeur, des mises à jour sont nécessaires afin de rétablir la connectivité du réseau. Une convergence lente des algorithmes de routage peut empêcher la livraison des données.

Les algorithmes de routage utilisent différentes métriques pour déterminer la meilleure route. 1

Protocole	Métrique	Nombre maximum de routeurs	Origines
Protocole RIP	Nombre de sauts	15	Xerox
Protocole IGRP	• Bande passante • Charge • Délai • Fiabilité	255	Cisco

Les métriques de routage sont les valeurs utilisées pour déterminer le meilleur chemin jusqu'au saut suivant.

Chacun d'eux interprète à sa façon ce qui est le mieux. L'algorithme génère un nombre, appelé valeur métrique, pour chaque chemin traversant le réseau. Les algorithmes de routage perfectionnés effectuent la sélection du chemin en fonction de plusieurs métriques combinées en une valeur composite. Généralement, les valeurs métriques faibles indiquent le meilleur chemin.

Les métriques peuvent être calculées sur la base d'une seule caractéristique de chemin, comme elles peuvent l'être sur la base de plusieurs. Les métriques les plus communément utilisées par les protocoles de routage sont les suivantes:

- **Bande passante:** la bande passante représente la capacité de débit d'une liaison. Une liaison Ethernet de 10 Mbits/s est généralement préférable à une ligne louée de 64 Kbits/s.
- **Délai:** le délai est le temps nécessaire à l'acheminement d'un paquet, pour chaque liaison, de la source à la destination. Il dépend de la bande passante des liaisons intermédiaires, de la quantité de données pouvant être temporairement stockées sur chaque routeur, de la congestion du réseau et de la distance physique.
- **Charge:** la charge est la quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison.
- **Fiabilité:** la fiabilité se rapporte habituellement au taux d'erreurs de chaque liaison du réseau.
- **Nombre de sauts:** le nombre de sauts est le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination. Chaque routeur équivaut à un saut. Un nombre de sauts égal à 4 signifie que les données doivent passer par quatre routeurs pour atteindre leur destination. Lorsque plusieurs chemins sont possibles, c'est le chemin comportant le moins de sauts qui est privilégié.
- **Tops:** délai d'une liaison de données utilisant les tops d'horloge d'un PC IBM, un top d'horloge correspondant environ à 1/18 seconde.
- **Coût:** le coût est une valeur arbitraire, généralement basée sur la bande passante, une dépense monétaire ou une autre mesure, attribuée par un administrateur réseau.

La page suivante présente deux types de protocoles de routage.

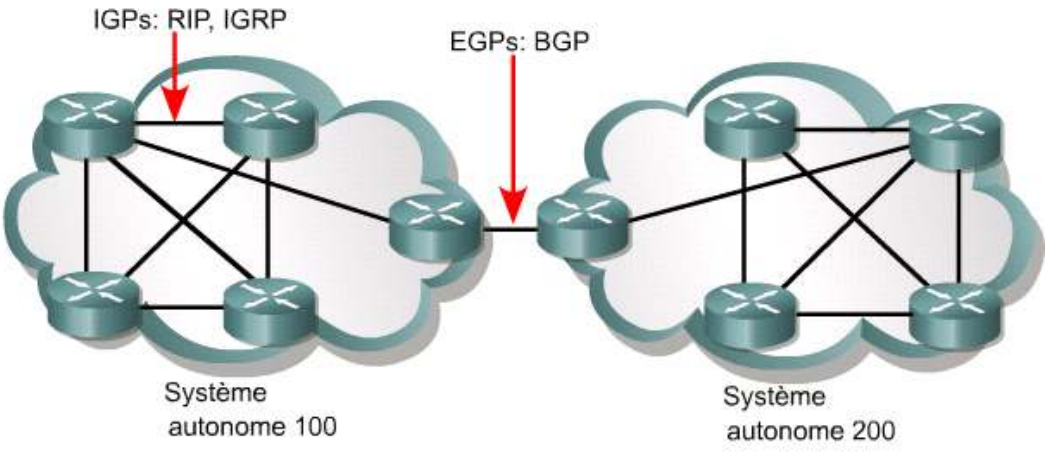
10.2 Protocoles de routage IP

10.2.7 Protocoles IGP et EGP

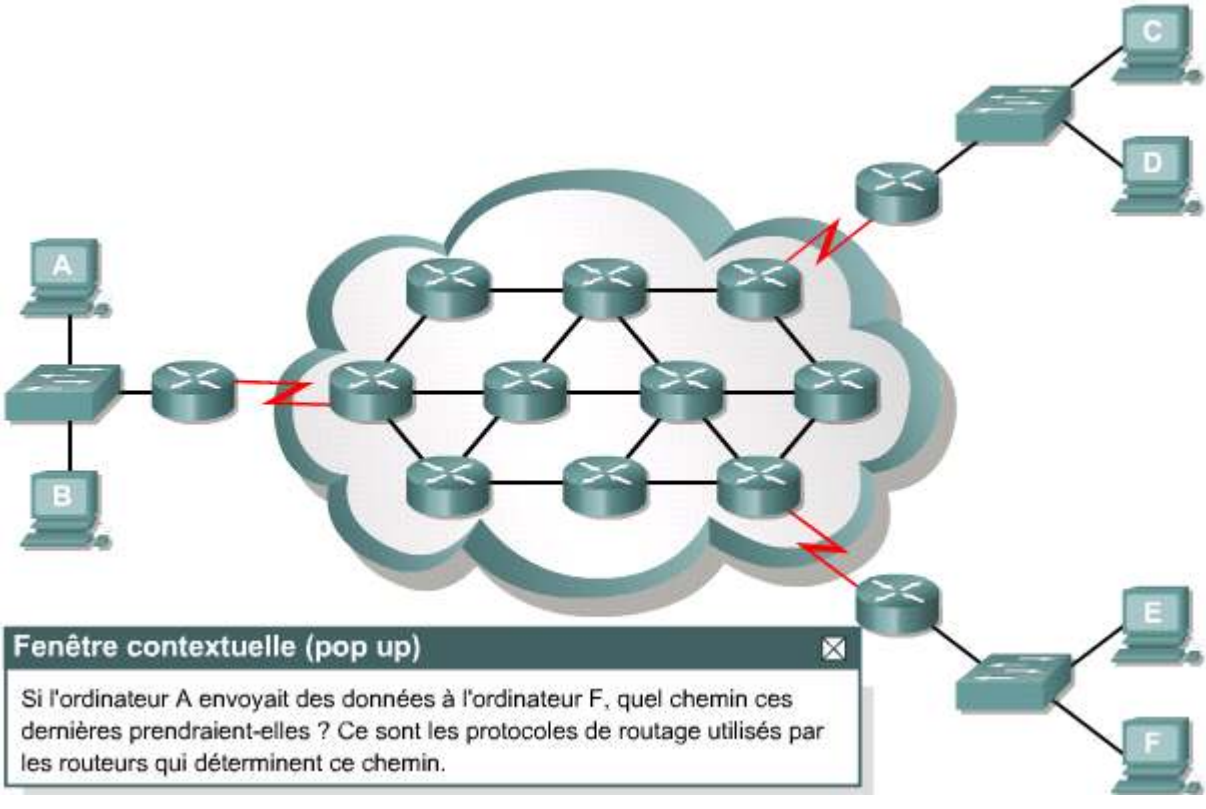
Cette page présente deux types de protocoles de routage.

Un système autonome est un réseau ou un ensemble de réseaux placés sous un même contrôle administratif, tel que le domaine cisco.com. Un tel système est constitué de routeurs qui présentent une vue cohérente du routage vers l'extérieur.

Il existe deux familles de protocoles de routage : les protocoles IGP (*Interior Gateway Protocol*) et les protocoles EGP (*Exterior Gateway Protocol*). 1 2



Un système autonome est un ensemble de réseaux placés dans un domaine administratif commun. Les protocoles IGP opèrent au sein d'un système autonome. Les protocoles EGP relient différents systèmes autonomes.


A
B
C
D
E
F
Fenêtre contextuelle (pop up)
Si l'ordinateur A envoyait des données à l'ordinateur F, quel chemin ces dernières prendraient-elles ? Ce sont les protocoles de routage utilisés par les routeurs qui déterminent ce chemin.

Les protocoles IGP acheminent les données au sein d'un système autonome. Il s'agit:

- Des protocoles RIP et RIPv2.
- Du protocole IGRP.
- Du protocole EIGRP.
- Du protocole OSPF.

- Du protocole IS-IS (*Intermediate System-to-Intermediate System*).

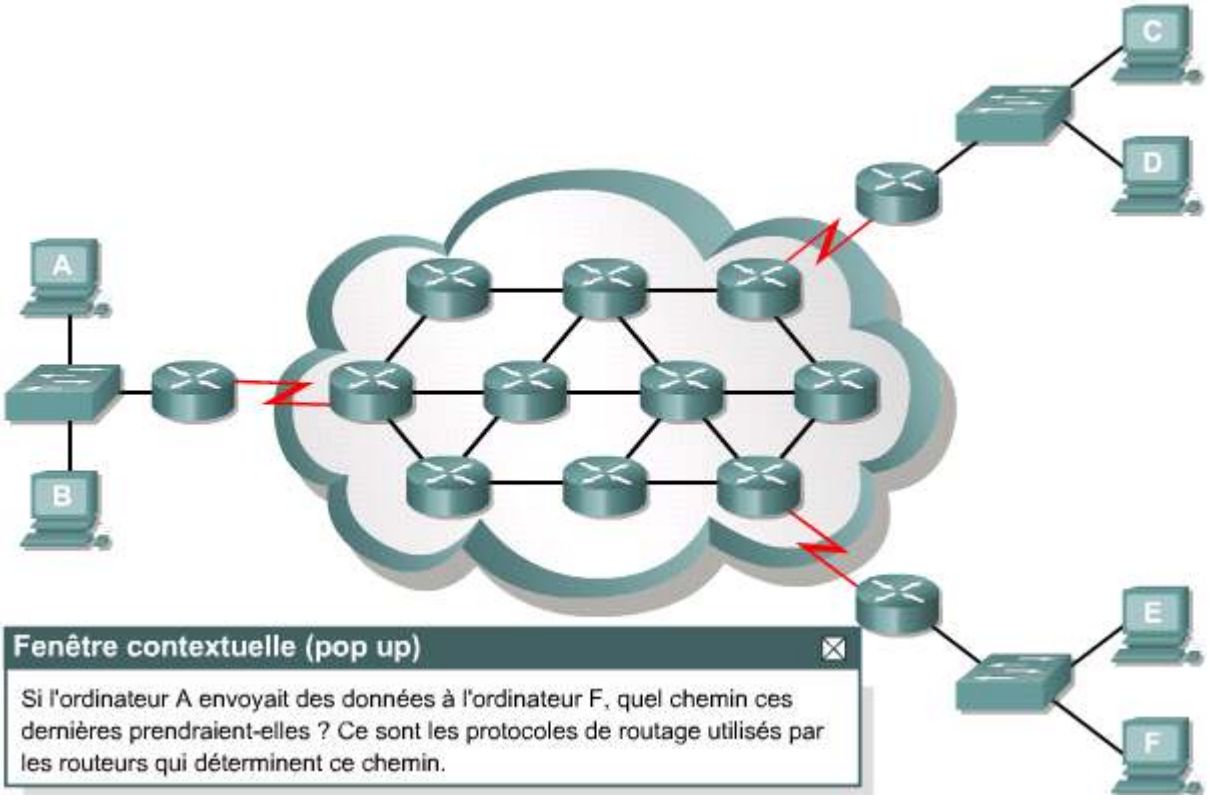
Les protocoles EGP acheminent les données entre les systèmes autonomes. Le protocole BGP est un exemple de ce type de protocole.

La page suivante explique ce que sont les protocoles à vecteur de distance et à état de liens.

10.2 Protocoles de routage IP

10.2.8 État de liens et vecteur de distance

Les protocoles de routage peuvent être classés en protocoles IGP ou EGP. Le type utilisé va dépendre de l'administration du groupe de routeurs, notamment s'ils sont placés sous une seule et même administration ou pas. Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens. 1


A
B
C
D
E
F
Fenêtre contextuelle (pop up)
Si l'ordinateur A envoyait des données à l'ordinateur F, quel chemin ces dernières prendraient-elles ? Ce sont les protocoles de routage utilisés par les routeurs qui déterminent ce chemin.

Cette page présente le routage à vecteur de distance et à état de liens, et explique quand ces différents types de protocoles de routage sont utilisés.

La méthode de routage à vecteur de distance détermine la direction (vecteur) et la distance vers n'importe quelle liaison de l'interréseau. La distance peut être représentée par le nombre de sauts vers cette liaison. Les routeurs faisant appel aux algorithmes de vecteur de distance envoient périodiquement l'intégralité ou une partie des entrées de leur table de routage aux routeurs adjacents, que des modifications aient été ou non apportées au réseau. Lorsqu'un routeur reçoit une mise à jour de routage, il vérifie tous les chemins connus et modifie le cas échéant sa propre table de routage. Ce processus est également appelé «routage par rumeur». La connaissance qu'a un routeur du réseau dépend de la vue dont dispose le routeur adjacent sur la topologie du réseau.

Les exemples suivants sont des exemples de protocoles à vecteur de distance:

- **Routing Information Protocol (RIP):** le protocole RIP est le protocole IGP le plus utilisé sur Internet. Son unique métrique de routage est basée sur le nombre de sauts.
- **Interior Gateway Routing Protocol (IGRP):** ce protocole IGP a été développé par Cisco afin de résoudre les problèmes associés au routage dans des réseaux hétérogènes étendus.
- **Enhanced IGRP (EIGRP):** ce protocole IGP, propriété de Cisco, inclut un grand nombre des caractéristiques d'un protocole de routage à état de liens. Il est, de ce fait, également appelé «protocole hybride symétrique», bien qu'il soit véritablement à classer dans les protocoles de routage à vecteur de distance avancés.

Les protocoles à état de liens ont été conçus pour pallier les limitations des protocoles de routage à vecteur de distance. Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue. Ces protocoles envoient par ailleurs des mises à jour périodiques, connues sous le nom d'actualisations à état de liens, à des intervalles moins fréquents, par exemple toutes les 30 minutes.

Dès qu'une unité a détecté la modification d'une liaison ou d'une route, elle crée une mise à jour de routage à état de liens (LSA, *link-state advertisement*) concernant cette liaison. Cette mise à jour LSA est ensuite transmise à tous les équipements voisins. Chacun d'eux en prend une copie, met à jour sa base de données à état de liens et transmet la mise à jour LSA aux autres unités voisines. Cette diffusion de mises à jour LSA est nécessaire afin que tous les équipements de routage puissent créer des bases de données transcrivant de manière précise la topologie du réseau et mettre à jour leur table de routage.

Les algorithmes à état de liens se servent généralement de leurs bases de données pour créer des entrées dans la table de routage qui privilégient le chemin le plus court. Les protocoles OSPF (*Open Shortest Path First*) et IS-IS (*Intermediate System-to-Intermediate System*) sont des exemples de protocoles à état de liens.

L'activité de média interactive souligne les différences entre les protocoles de routage à vecteur de distance et les protocoles à état de liens.

La page suivante fait le point sur les protocoles de routage.



Activité de média interactive

Case à cocher: Protocoles de routage à état de liens et à vecteur de distance

À l'issue de cette activité, les étudiants seront capables de faire la distinction entre les protocoles de routage à état de liens et les protocoles à vecteur de distance.

10.2 Protocoles de routage IP

10.2.9 Protocoles de routage

Cette page présente différents types de protocoles de routage.

Le protocole RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer la direction et la distance vers n'importe quelle liaison de l'interréseau. S'il existe plusieurs chemins vers une destination, le protocole RIP sélectionne celui qui comporte le moins de sauts. Toutefois, le nombre de sauts étant la seule métrique de routage utilisée par ce protocole, il ne sélectionne pas toujours le chemin le plus rapide. En outre, le protocole RIP ne peut acheminer un paquet au-delà de 15 sauts. La version 1 du protocole RIP (RIPv1) n'incluant pas les informations de masque de sous-réseau dans les mises

à jour de routage, tous les équipements du réseau doivent nécessairement utiliser le même masque de sous-réseau. On parle dans ce cas de routage par classes. 1

La version 2 (RIPv2) fournit un routage par préfixe et envoie les informations de masque de sous-réseau dans ses mises à jour de routage. On parle ici de routage sans classe. Avec les protocoles de routage sans classe, les sous-réseaux d'un même réseau peuvent comporter des masques différents. Cette technique fait référence à l'utilisation de masques de sous-réseau de longueur variable (VLSM).

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il a été spécifiquement développé pour résoudre les problèmes associés au routage dans de grands réseaux qui dépassaient la portée des protocoles tels que RIP. IGRP peut sélectionner le chemin disponible le plus rapide en fonction du délai, de la bande passante, de la charge et de la fiabilité. Le nombre de sauts maximal autorisé est par ailleurs considérablement plus élevé que celui défini dans le protocole RIP. Le protocole IGRP utilise uniquement le routage par classes.

Le protocole OSPF est un protocole de routage à état de liens mis au point par l'IETF (*Internet Engineering Task Force*) en 1988. Il a été écrit pour permettre la gestion de vastes interréseaux évolutifs hors de portée du protocole RIP.

Le protocole IS-IS (*Intermediate System-to-Intermediate System*) est un protocole de routage à état de liens utilisé pour les protocoles routés autres qu'IP. Il existe une extension du protocole IS-IS, Integrated IS-IS, qui, elle, prend en charge plusieurs protocoles routés dont IP.

À l'instar du protocole IGRP, EIGRP est un protocole développé par Cisco. Il constitue une version perfectionnée du protocole IGRP. Plus précisément, ce protocole offre de meilleures performances d'exploitation comme une convergence plus rapide et une bande passante moins surchargée. C'est un protocole à vecteur de distance avancé qui a également recours à certaines fonctions des protocoles à état de liens. Il est, par conséquent, parfois classé dans les protocoles de routage hybrides.

Le protocole BGP (*Border Gateway Protocol*) est un exemple de protocole EGP (*External Gateway Protocol*). Il permet l'échange d'informations de routage entre systèmes autonomes tout en garantissant une sélection de chemins exempts de boucle. Le protocole BGP est le protocole de mises à jour de routage le plus utilisé par les grandes sociétés et les FAI sur Internet. BGP4 est la première version de BGP à prendre en charge le routage interdomaine sans classes (CIDR) et le regroupement de routes. À la différence des protocoles IGP courants, comme RIP, OSPF et EIGRP, le protocole BGP ne se sert pas de métriques tels que le nombre de sauts, la bande passante ou le délai. Il prend à la place ses décisions de routage selon des stratégies de réseau (ou règles utilisant divers attributs de chemin BGP).

Au cours de l'exercice de TP, les étudiants pourront se faire une idée du prix d'un petit routeur.

Cette page termine la leçon. La leçon suivante portera sur le découpage en sous-réseaux. La première page aborde les différentes classes d'adresses IP.

Activité de TP

Exercice: Achat d'un petit routeur

Ce TP a pour objectif de vous présenter les divers composants de réseau existant sur le marché, ainsi que leur prix. Il couvre plus précisément les petits routeurs utilisés par les télétravailleurs.

10.3 Mécanisme de découpage en sous-réseaux

Cette page permet de revoir les classes d'adresses IP. La combinaison des différentes classes d'adresses IP offre une plage d'hôtes comprise entre 256 et 16,8 millions.

Pour permettre une gestion efficace d'un nombre limité d'adresses IP, il est possible de subdiviser toutes les classes en sous-réseaux plus petits. La figure 1

Classe A	Réseau	Hôte		
Octet	1	2	3	4

Classe B	Réseau		Hôte	
Octet	1	2	3	4

Classe C	Réseau			Hôte
Octet	1	2	3	4

Classe D	Hôte			
Octet	1	2	3	4

Les adresses de classe D sont utilisées pour les groupes de multicast. Il n'est pas nécessaire d'allouer des octets ou des bits pour séparer les adresses réseau et hôte. Les adresses de classe E sont réservées à la recherche.

donne une vue d'ensemble de la division réseaux-hôtes.

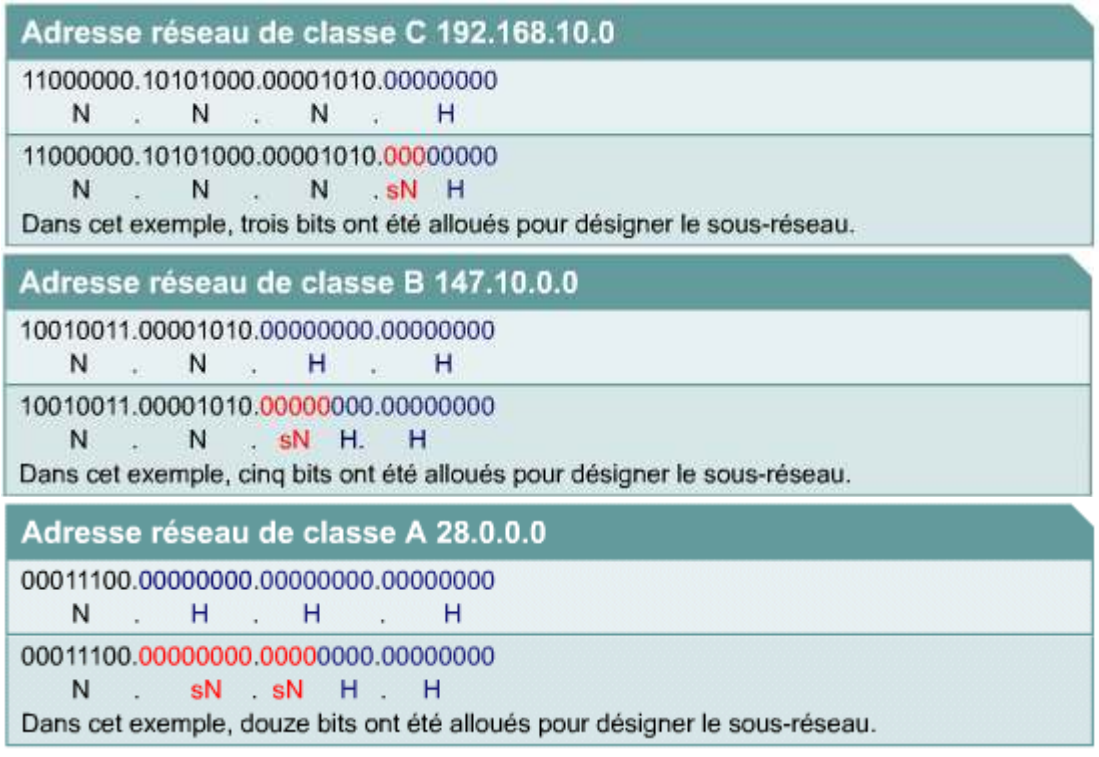
La page suivante explique l'importance du découpage en sous-réseaux.

10.3 Mécanisme de découpage en sous-réseaux
10.3.2 Introduction au découpage en sous-réseaux

Cette page explique le mécanisme du découpage en sous-réseaux (subnetting) et son importance.

Pour effectuer un découpage en sous-réseaux, des bits de la partie hôte doivent être réattribués au réseau. Cette opération est souvent appelée « emprunt » de bits. Il serait en fait plus juste de parler de « prêt ». L'emprunt se fait toujours à partir du bit d'hôte situé le plus à gauche, à savoir celui le plus proche du dernier octet de la partie réseau.

Les adresses de sous-réseau contiennent une partie réseau de classe A, B ou C, plus un champ de sous-réseau et un champ d'hôte. Le champ de sous-réseau et le champ d'hôte sont créés à partir de la partie hôte d'origine de l'adresse IP principale. Cette opération s'effectue en réattribuant des bits de la partie hôte à la partie réseau d'origine de l'adresse. 1 – 3


Adresse réseau de classe C 192.168.10.0
11000000.10101000.00001010.00000000
N . N . N . H
11000000.10101000.00001010.00000000
N . N . N . sN H
Dans cet exemple, trois bits ont été alloués pour désigner le sous-réseau.
Adresse réseau de classe B 147.10.0.0
10010011.00001010.00000000.00000000
N . N . H . H
10010011.00001010.00000000.00000000
N . N . sN H. H
Dans cet exemple, cinq bits ont été alloués pour désigner le sous-réseau.
Adresse réseau de classe A 28.0.0.0
00011100.00000000.00000000.00000000
N . H . H . H
00011100.00000000.00000000.00000000
N . sN . sN H . H
Dans cet exemple, douze bits ont été alloués pour désigner le sous-réseau.

Le fait de pouvoir diviser la partie hôte d'origine de l'adresse en nouveaux champs de sous-réseau et d'hôte permet à l'administrateur réseau de gagner en flexibilité au niveau de l'adressage.

En plus de faciliter la gestion du réseau, le découpage en sous-réseaux permet à l'administrateur réseau de confiner le broadcast et de garantir une certaine sécurité sur le réseau LAN. Ce dernier point est rendu possible du fait que l'accès aux autres sous-réseaux ne peut se faire qu'à travers les services d'un routeur. Les accès peuvent par ailleurs être sécurisés grâce à l'utilisation de listes de contrôle d'accès qui autorisent ou refusent l'accès à un sous-réseau en fonction de plusieurs critères. Ces listes feront l'objet d'une étude plus loin dans le cursus. Certains propriétaires de réseaux de classes A et B ont également découvert que le découpage en sous-réseaux était source de revenus du fait de la vente ou de la location d'adresses IP jusqu'alors inutilisées.

Le découpage en sous-réseaux est une opération purement interne à un réseau. Vu de l'extérieur, un réseau LAN est un réseau unique qui ne donne aucune information sur sa structure interne. Cette perspective permet de conserver des tables de routage de petite taille et efficaces. Supposons l'adresse de nœud locale 147.10.43.14 sur le sous-réseau 147.10.43.0. À l'extérieur du réseau LAN, seul le numéro de réseau principal 147.10.0.0 est visible. La raison en est simple : l'adresse de sous-réseau locale 147.10.43.0 n'est valable qu'au sein du réseau LAN subdivisé en sous-réseaux.

La page suivante aborde les masques de sous-réseau.

10.3 Mécanisme de découpage en sous-réseaux

10.3.3 Détermination de l'adresse d'un masque de sous-réseau

Cette page contient des informations détaillées sur les masques de sous-réseau et explique comment ils sont établis.

Le nombre de bits à sélectionner dans le processus de découpage en sous-réseaux dépend du nombre maximal d'hôtes requis par sous-réseau. Pour calculer le nombre de sous-réseaux et d'hôtes créés par l'emprunt de bits, il

est nécessaire d'avoir des notions de base en calculs binaires et de connaître la valeur de position des bits dans un octet. 1

Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1

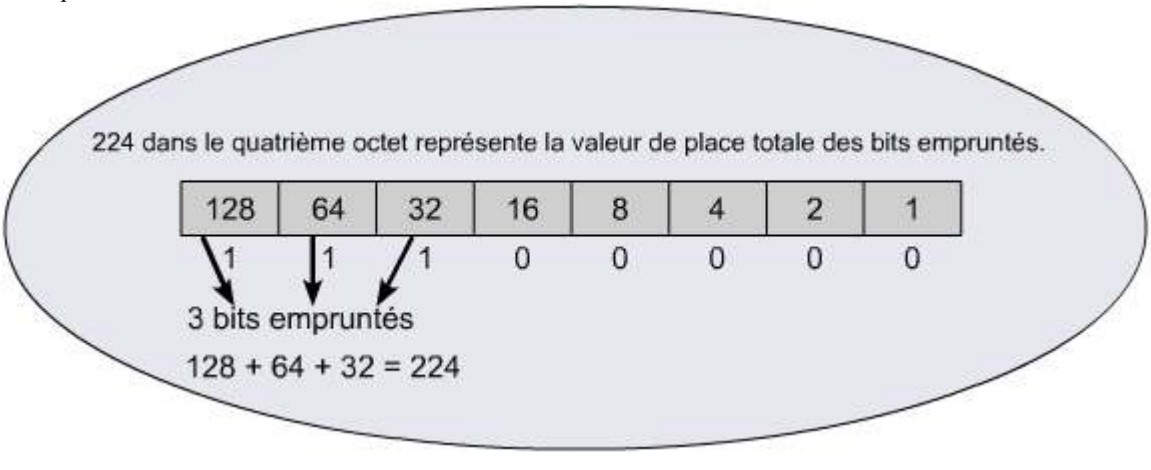
Quelle que soit la classe d'adresse IP, les deux derniers bits du dernier octet ne doivent jamais être attribués au sous-réseau. Ces bits constituent les deux derniers bits significatifs. Si vous utilisez tous les bits disponibles, à l'exception de ces deux derniers, pour créer des sous-réseaux, les sous-réseaux créés ne comporteront que deux hôtes utilisables. Il s'agit d'une méthode de conservation d'adresses pratique pour l'adressage des liaisons de routeur série. Toutefois, pour un réseau LAN effectif, cela impliquerait des coûts en équipement dépassant l'entendement.

Le masque de sous-réseau apporte au routeur l'information dont il a besoin pour déterminer le réseau et le sous-réseau auxquels un hôte donné appartient. 2

Slash format	/25	/26	/27	/28	/29	/30	N/A	N/A
Mask	128	192	224	240	248	252	254	255
Bits borrowed	1	2	3	4	5	6	7	8
Value	128	64	32	16	8	4	2	1

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

Le masque de sous-réseau est créé en utilisant des 1 dans les positions binaires du réseau. Les bits du sous-réseau sont déterminés en ajoutant la valeur de position des bits empruntés. Ainsi, si trois bits sont empruntés, le masque d'une adresse de classe C donne 255.255.255.224. 3


224 dans le quatrième octet représente la valeur de place totale des bits empruntés.
128 64 32 16 8 4 2 1
1 1 1 0 0 0 0 0
3 bits empruntés
128 + 64 + 32 = 224

Au format de barre oblique, ce masque est représenté par /27. Le nombre situé après la barre oblique correspond au nombre total de bits utilisés pour les parties réseau et sous-réseau.

Pour savoir combien de bits doivent être utilisés, le concepteur du réseau doit d'abord calculer le nombre d'hôtes nécessaires à son sous-réseau le plus vaste ainsi que le nombre de sous-réseaux requis. Supposons que le réseau requiert six sous-réseaux de 25 hôtes chacun. La méthode la plus simple pour déterminer le nombre de

bits à réaffecter est de se reporter au tableau de découpage en sous-réseaux.

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de sous-réseaux		4	8	16	32	64		
Sous-réseaux utilisables		2	6	14	30	62		
Nombre total d'hôtes		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

Si vous consultez la ligne intitulée " Sous-réseaux utilisables ", vous constatez que trois bits doivent être empruntés au champ d'hôte pour donner une possibilité de 6 sous-réseaux utilisables. Le tableau vous informe également que 30 hôtes utilisables sont alors disponibles pour chaque sous-réseau créé, ce qui répond tout à fait à vos besoins actuels. Il existe une différence entre les hôtes utilisables et le nombre total d'hôtes qui tient à l'utilisation de deux adresses spécifiques pour chaque sous-réseau : l'ID du réseau (représenté par la première adresse disponible) et l'adresse de broadcast (représentée par la dernière adresse disponible). Savoir emprunter le nombre de bits appropriés nécessaires aux sous-réseaux et aux hôtes de chacun des sous-réseaux constitue un exercice périlleux qui peut être à l'origine d'un certain nombre d'adresses hôtes inutilisées dans les divers sous-réseaux. Le routage par classes ne permet pas de limiter la perte de ces adresses. En revanche, le routage sans classe (qui sera abordé un peu plus loin dans ce cours) peut vous aider à récupérer un bon nombre de ces adresses perdues.

Pour résoudre les problèmes liés à la subdivision en sous-réseaux, vous pouvez faire appel à la même méthode que celle utilisée pour la création du tableau des sous-réseaux. Cette méthode se base sur la formule suivante :

Nombre de sous-réseaux utilisables = deux à la puissance du nombre de bits attribués au sous-réseau ou nombre de bits empruntés, moins deux. La soustraction correspond aux deux adresses réservées que sont l'adresse du réseau et l'adresse de broadcast du réseau.

$(2^{\text{nombre de bits empruntés}}) - 2 =$ sous-réseaux utilisables

$(2^3) - 2 = 6$

Nombre d'hôtes utilisables = deux à la puissance des bits restants, moins deux (pour les adresses réservées que sont l'adresse du sous-réseau et l'adresse de broadcast du sous-réseau).

$(2^{\text{nombre de bits hôtes restants}}) - 2 =$ hôtes utilisables

$(2^5) - 2 = 30$

La page suivante explique l'application d'un masque de sous-réseau.

10.3 Mécanisme de découpage en sous-réseaux
10.3.4 Application du masque de sous-réseau

Cette page explique aux étudiants comment appliquer un masque de sous-réseau.

Une fois le masque de sous-réseau défini, vous pouvez l'utiliser pour établir le modèle de sous-réseau. Le tableau de la figure 1

Numéro du sous-réseau	ID du sous-réseau	Plage d'hôtes	ID de broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

donne un exemple du nombre de sous-réseaux et d'adresses qui peuvent être créés en attribuant trois bits au champ de sous-réseau. Cela permet en fait de créer huit sous-réseaux comportant chacun 32 hôtes. La numérotation des sous-réseaux commence à zéro (0), et le premier sous-réseau est donc toujours le sous-réseau zéro.

Le remplissage du tableau se fait automatiquement pour trois de ses champs mais demande quelques calculs pour les autres. L'adresse du sous-réseau zéro est identique à celle du réseau principal, ici 192.168.10.0. L'adresse de broadcast pour l'ensemble du réseau est le nombre le plus élevé, soit 192.168.10.255 dans notre cas. Le troisième nombre directement obtenu est l'ID du sous-réseau numéro sept. Il est constitué des trois octets du réseau et du numéro de masque de sous-réseau inséré au niveau du quatrième octet. Trois bits ont été attribués au champ de sous-réseau donnant la valeur 224. 2

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de sous-réseaux		4	8	16	32	64		
Sous-réseaux utilisables		2	6	14	30	62		
Nombre total d'hôtes		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

L'ID du sous-réseau 7 est 192.168.10.224. L'insertion de ces nombres entraîne la définition de points de contrôle qui vérifieront l'exactitude du tableau une fois celui-ci complété.

En consultant le tableau de découpage en sous-réseaux ou en appliquant la formule, on constate que les trois bits attribués au champ de sous-réseau donne un résultat total de 32 hôtes dans chacun des sous-réseaux. 2 À partir de ces informations, vous pouvez calculer l'adresse de chacun des sous-réseaux. Il vous suffit en effet d'ajouter 32 à chacun des numéros précédents, en commençant par le sous-réseau zéro. 1 Notez que la partie hôte de l'adresse de sous-réseau ne comporte que des bits à 0.

Le champ de broadcast est le dernier numéro de chaque sous-réseau et il ne comporte que des 1 dans la partie hôte. Cette adresse ne permet la diffusion que vers les hôtes d'un même sous-réseau. 1 L'adresse du sous-réseau zéro étant 192.168.10.0 et le nombre total d'hôtes s'élevant à 32 hôtes, l'adresse de broadcast est la suivante : 192.168.10.31. En effet, si l'on commence à calculer à partir de zéro, le 32ème numéro séquentiel est le numéro 31. Il est important de garder à l'esprit qu'en gestion de réseaux, zéro (0) constitue un vrai nombre.

Vous pouvez renseigner la colonne relative à l'adresse de broadcast de la même manière que vous avez indiqué l'adresse des sous-réseaux. Ajoutez simplement 32 à l'adresse de broadcast précédente du sous-réseau. Une autre méthode consiste à partir du bas de cette colonne et à remonter vers le haut en soustrayant 1 de l'adresse de sous-réseau précédente.

La page suivante aborde le découpage en sous-réseaux des réseaux de classe A, B et C.

10.3 Mécanisme de découpage en sous-réseaux

10.3.5 Découpage de réseaux de classe A et B en sous-réseaux

Cette page décrit le processus utilisé pour subdiviser les réseaux de classes A, B et C en sous-réseaux.

La méthode de découpage en sous-réseaux des réseaux de classes A et B est identique à celle utilisée pour les réseaux de classe C, à l'exception du nombre de bits impliqués qui est considérablement plus élevé. Le nombre de bits disponibles à attribuer au champ de sous-réseau dans une adresse de classe A est de 22 bits, tandis qu'il

est de 14 bits pour une adresse de classe B. 1 2

Adresse réseau de classe B 147.10.0.0 (14 bits disponibles)

10010011.00001010.00000000.00000000
N . N . H . H

10010011.00001010.00000000.00000000
N . N . sN . sN H

Dans cet exemple, 12 bits ont été alloués pour désigner le sous-réseau.

Adresse réseau de classe A 28.0.0.0 (22 bits disponibles)

00011100.00000000.00000000.00000000
N . H . H . H

00011100.00000000.00000000.00000000
N . sN . sN . sN H

Dans cet exemple, 20 bits ont été alloués pour désigner le sous-réseau.

En attribuant 12 bits d'une adresse de classe B au champ de sous-réseau, vous créez le masque de sous-réseau 255.255.255.240 ou /28. L'ensemble des huit bits ont été attribués dans le troisième octet donnant 255, la valeur totale des huit bits. Quatre bits ont été attribués dans le quatrième octet donnant le résultat 240. Petit rappel : le masque de format /# correspond à la somme totale des bits attribués au champ de sous-réseau en plus des bits fixes du réseau. 3

Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Sous-réseaux	2	4	8	16	32	64	128	256

Une adresse de classe C avec le masque /25 emprunte uniquement un bit, comme indiqué dans le tableau ci-dessus. Toutefois, une adresse de classe B avec le même masque va emprunter neuf bits.

L'attribution de 20 bits d'une adresse de classe A au champ de sous-réseau crée le masque de sous-réseau 255.255.255.240 ou /28. L'ensemble des huit bits des deuxième et troisième octets sont affectés au champ de sous-réseau, ainsi que quatre bits du quatrième octet.

Ici, il apparaît clairement que les masques de sous-réseau des adresses de classes A et B sont identiques. À moins d'associer le masque à une adresse réseau, il est impossible de savoir combien de bits ont été affectés au sous-réseau. 4 5

Deux à la puissance de	égale
0	1
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192
14	16384
15	32768
16	65536
17	131072
18	262144
19	524288
20	1048576
21	2097152
22	4194304

Entrez la valeur du masque de sous-réseau dans la zone correspondante en fonction des informations fournies dans les autres champs. Vérifiez la réponse en cliquant sur le bouton correspondant.

Adresse réseau	104.0.0.0
Nombre de sous-réseaux utilisables	56
Nombre d'hôtes par sous-réseau	10
Masque de sous-réseau	

Vérifiez votre réponse

Entrez la valeur du masque de sous-réseau dans la zone correspondante en fonction des informations fournies dans les autres champs. Vérifiez la réponse en cliquant sur le bouton correspondant.

Adresse réseau	11.0.0.0
Nombre de sous-réseaux utilisables	143
Nombre d'hôtes par sous-réseau	10
Masque de sous-réseau	255.255.0.0

Vérifiez votre réponse

Correct

Réessayer

- (•) ClassA
- ( ) ClassB
- ( ) ClassC
- ( ) All Classes

Quelle que soit la classe sur laquelle porte la subdivision, les règles sont les mêmes:

Nombre total de sous-réseaux = $2^{\text{nombre de bits empruntés}}$

Nombre total d'hôtes = $2^{\text{nombre de bits restants}}$

Sous-réseaux utilisables = $2^{\text{nombre de bits empruntés}}$ **moins 2**

Hôtes utilisables = $2^{\text{nombre de bits restants}}$ **moins 2**

La page suivante explique l'opération AND logique.

Activité de TP

Exercice: Notions de base sur le découpage en sous-réseaux

Ce TP a pour objectif d'identifier l'utilité d'un masque de sous-réseau et de distinguer un masque de sous-réseau par défaut d'un masque personnalisé.

Activité de TP

Exercice: Découpage d'un réseau de classe A en sous-réseaux

Ce TP a pour objectif l'analyse d'une adresse réseau de classe A avec le nombre de bits réseau indiqués afin de déterminer les éléments suivants : le masque de sous-réseau, le nombre de sous-réseaux, le nombre d'hôtes par sous-réseau et des informations sur des sous-réseaux spécifiques.

Activité de TP

Exercice: Découpage d'un réseau de classe B en sous-réseaux

Ce TP a pour objectif de fournir un schéma de découpage en sous-réseaux à partir d'une adresse réseau de classe B.

Activité de TP

Exercice: Découpage d'un réseau de classe C en sous-réseaux

Ce TP a pour objectif de fournir un schéma de découpage en sous-réseaux à partir d'une adresse réseau de classe C.

10.3 Mécanisme de découpage en sous-réseaux

10.3.6 Calcul du sous-réseau via l'opération AND

Cette page explique en quoi consiste l'opération AND.

Les routeurs se servent des masques de sous-réseau pour déterminer le sous-réseau de chacun des nœuds. On parle alors d'opération AND logique. Il s'agit d'un processus binaire par lequel le routeur calcule l'ID de sous-réseau d'un paquet entrant. 1

0	AND	0	=	0
0	AND	1	=	0
1	AND	0	=	0
1	AND	1	=	1

L'opération AND est similaire à une multiplication.

Ce processus s'effectue au niveau binaire. Il est par conséquent nécessaire d'afficher l'adresse IP et le masque au format binaire. 2

Adresse du paquet	201.10.11.65	11001001.00001010.00001011.01000001
AND		
Masque	255.255.255.224	11111111.11111111.11111111.11100000
ID du sous-réseau	201.10.11.64	11001001.00001010.00001011.01000000

L'opération AND est appliquée à l'adresse IP et à l'adresse du sous-réseau avec pour résultat l'ID du sous-réseau. Cette information permet au routeur de transférer le paquet à l'interface appropriée.

Le découpage en sous-réseaux est une opération qui s'apprend. Il vous faudra vous exercer de nombreuses heures avant de pouvoir développer des systèmes flexibles et exploitables. Vous pouvez trouver de nombreux outils de calcul de sous-réseaux sur le Web. Un administrateur réseau se doit cependant de savoir créer

manuellement ces sous-réseaux afin de pouvoir élaborer de manière efficace le système de réseaux adéquat et de pouvoir vérifier la validité des résultats d'un outil de calcul. Ce dernier se contente en effet de fournir le système d'adressage final, sans indiquer le système initial. En outre, l'utilisation d'outils de calcul, quels qu'ils soient, est interdite pendant l'examen de certification.

Cette page termine la leçon. La page suivante récapitule les principaux points évoqués au cours de ce module.

Résumé

Cette page résume les sujets traités dans ce module.

Le protocole IP est dit protocole non orienté connexion parce qu'aucune connexion à un circuit dédié n'est établie entre la source et la destination avant la transmission. Il est considéré comme non fiable car il ne vérifie pas la bonne livraison des données. S'il est nécessaire de vérifier la bonne livraison des données, il faut combiner le protocole IP à un protocole de transport orienté connexion, tel que TCP. S'il n'est pas nécessaire de vérifier l'intégrité des données à la livraison, IP peut être utilisé avec un protocole sans connexion, tel que UDP. Les processus réseau sans connexion sont souvent appelés processus à commutation de paquets, tandis que les processus réseau orientés connexion sont dits processus à commutation de circuits.

Les protocoles ajoutent des informations de contrôle aux données au niveau de chaque couche du modèle OSI tout au long de leur transmission sur le réseau. Ces informations étant ajoutées au début et à la fin des données, on parle d'encapsulation des données. La couche 3 ajoute des informations d'adresse réseau ou logique aux données et la couche 2 des informations d'adresse locale ou physique.

Le routage de la couche 3 et la commutation de la couche 2 permettent d'acheminer et de livrer les données sur le réseau. Au départ, le routeur reçoit une trame de couche 2 avec un paquet de couche 3 encapsulé en son sein. Il doit retirer la trame de couche 2 et examiner le paquet de couche 3. Si ce dernier est destiné à une adresse locale, le routeur doit l'encapsuler dans une nouvelle trame dotée de la bonne adresse MAC locale de destination. Si les données doivent être transmises vers un autre domaine de broadcast, le routeur encapsule le paquet de couche 3 dans une nouvelle trame de couche 2 contenant l'adresse MAC de l'unité d'interconnexion de réseaux suivante. La trame est ainsi transférée sur le réseau de domaine de broadcast en domaine de broadcast jusqu'à sa livraison finale à l'hôte approprié.

Les protocoles routés, comme IP, transportent les données sur un réseau. Les protocoles de routage, quant à eux, permettent aux routeurs de choisir le meilleur chemin pour acheminer les données de la source à leur destination. Ce chemin peut être une route statique, entrée manuellement, ou une route dynamique, connue par le biais des protocoles de routage. Dans le cas du routage dynamique, les routeurs s'échangent des mises à jour de routage afin de gérer leur table. Les algorithmes de routage mettent en œuvre des métriques pour traiter les mises à jour de routage et informer les tables de routage des meilleurs chemins possibles. La convergence décrit la vitesse à laquelle tous les routeurs acquièrent une même vue du réseau après qu'il ait subi une modification.

Les protocoles IGP (*Interior Gateway Protocol*) sont des protocoles de routage qui acheminent les données au sein de systèmes autonomes, tandis que les protocoles EGP (*Exterior Gateway Protocol*) acheminent les données entre les différents systèmes autonomes. Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens. Les routeurs faisant appel aux protocoles à vecteur de distance envoient périodiquement des mises à jour de routage constituées de l'intégralité ou d'une partie de leur table de routage. Les routeurs utilisant les protocoles à état de liens, pour leur part, se servent des mises à jour de routage à état de liens (LSA) pour envoyer des mises à jour uniquement lorsque des modifications surviennent dans la topologie du réseau. Ils peuvent en outre, mais moins fréquemment, envoyer les tables de routage complètes.

Lors de la transmission des paquets sur le réseau, il est nécessaire que les unités puissent distinguer la partie réseau de la partie hôte de l'adresse IP. Un masque d'adresse de 32 bits, appelé masque de sous-réseau, permet d'indiquer les bits d'une adresse IP utilisés pour l'adresse réseau. Le masque de sous-réseau par défaut pour une adresse de classe A est 255.0.0.0. Pour une adresse de classe B, le masque de sous-réseau commence toujours

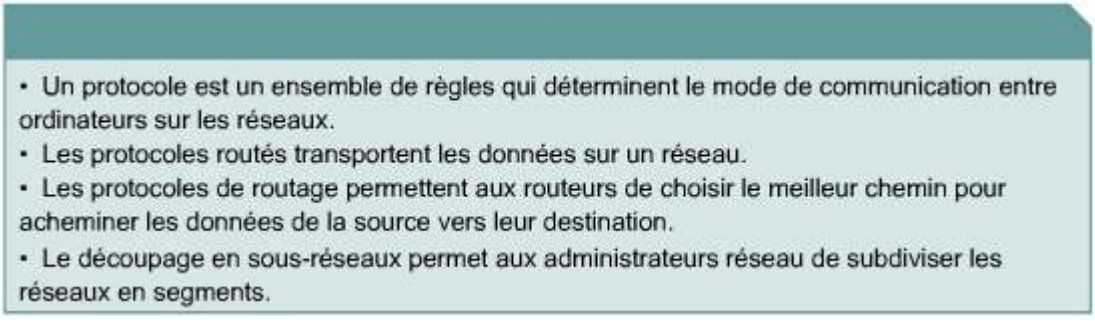
par 255.255.0.0 et celui d'une adresse de classe C par 255.255.255.0. Le masque de sous-réseau peut être utilisé pour diviser un réseau existant en plusieurs « sous-réseaux ».

Le découpage d'un réseau en sous-réseaux permet de réduire la taille des domaines de broadcast, permet aux segments LAN situés dans plusieurs zones géographiques différentes de communiquer par le biais de routeurs et améliore la sécurité en isolant les segments LAN les uns des autres.

Les masques de sous-réseau personnalisés utilisent plus de bits que les masques par défaut en les empruntant à la partie hôte de l'adresse IP. Une adresse en trois parties est ainsi créée:

- L'adresse réseau d'origine;
- L'adresse de sous-réseau composée des bits empruntés;
- L'adresse hôte composée des bits restants après l'emprunt des bits servant à créer les sous-réseaux.

Les routeurs utilisent les masques de sous-réseau pour déterminer la partie sous-réseau d'une adresse d'un paquet entrant. On parle alors d'opération AND logique.


• Un protocole est un ensemble de règles qui déterminent le mode de communication entre ordinateurs sur les réseaux.
• Les protocoles routés transportent les données sur un réseau.
• Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin pour acheminer les données de la source vers leur destination.
• Le découpage en sous-réseaux permet aux administrateurs réseau de subdiviser les réseaux en segments.

11-La couche transport et couche application de protocole TCP/IP

Vue d'ensemble

La couche transport du modèle TCP/IP achemine les données entre les applications des machines source et de destination. Pour comprendre les réseaux de données actuels, il est capital de bien connaître le mécanisme de la couche transport. Ce module a pour objectif de décrire les fonctions et les services de cette couche.

Bon nombre des applications réseau intervenant au niveau de la couche application TCP/IP sont déjà connues des utilisateurs des réseaux. Les acronymes HTTP, FTP et SMTP sont familiers aux utilisateurs de navigateurs Web et de clients de messagerie. Ce module présente également le rôle de ces applications, entre autres, du modèle de réseau TCP/IP.

Ce module se rapporte à des objectifs spécifiques des examens de certification CCNA 640-801, INTRO 640-821 et ICND 640-811. 2 3 4

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
			• Évaluation du processus de communication TCP/IP et de ses protocoles associés • Description des communications réseau à l'aide des modèles en couche • Évaluation des règles de gestion des paquets

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
			• Évaluation des règles de gestion des paquets

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Évaluation des règles de gestion des paquets • Description de l'impact des protocoles associés à TCP/IP sur la communication des hôtes • Description des principes et de l'usage de la commutation de paquets utilisant le protocole IP (Internet Protocol)

À l'issue de ce module, les étudiants seront en mesure d'effectuer les actions suivantes: 1

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
11.1	Couche transport TCP/IP
11.2	Couche application

- Décrire les fonctions de la couche transport du modèle TCP/IP.
- Expliquer le contrôle de flux.
- Expliquer la connexion entre systèmes homologues.
- Décrire le fenêtrage.
- Décrire le mécanisme d'accusés de réception.
- Identifier et présenter les protocoles de la couche transport.
- Décrire les formats d'en-tête TCP et UDP.
- Décrire les numéros de port TCP et UDP.
- Énumérer les principaux protocoles de la couche application TCP/IP.
- Exposer les fonctions et le mécanisme des applications TCP/IP bien connues.

11.1 Couche transport TCP/IP

11.1.1 Introduction à la couche transport

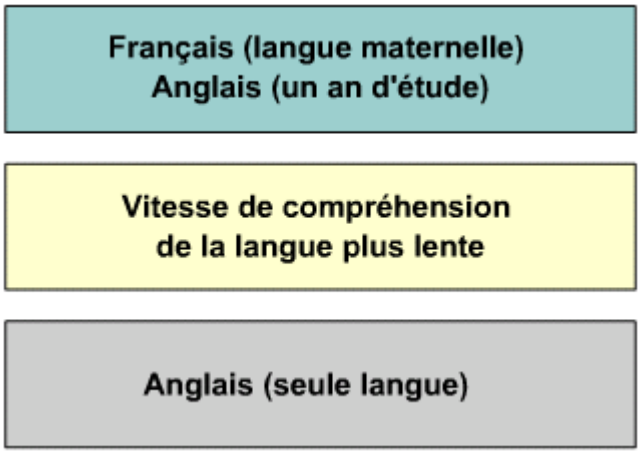
Cette page présente les fonctions de la couche transport. 1

Un transport fiable exécute les opérations suivantes :

- Garantir qu'un accusé de réception sera envoyé à l'expéditeur des segments.
- Assurer la retransmission des segments qui n'ont pas été reçus.
- Transmettre à l'unité de destination les segments dans l'ordre approprié.
- Éliminer la congestion et assurer un contrôle.

Le rôle principal de la couche transport est d'acheminer et de contrôler le flux d'informations de la source à la destination, de manière fiable et précise. Le contrôle de bout en bout ainsi que la fiabilité sont assurés grâce aux fenêtres glissantes, aux numéros de séquence et aux accusés de réception.

Pour mieux comprendre les concepts de fiabilité et de contrôle de flux, imaginez une personne qui apprend une langue étrangère pendant un an avant de se rendre dans le pays en question. Au cours d'une conversion, certains mots seront répétés pour assurer la fiabilité de la compréhension. Les interlocuteurs doivent par ailleurs parler lentement afin de se faire comprendre, ce qui peut être associé au contrôle de flux. 2



La couche transport établit une connexion logique entre deux points d'extrémité d'un réseau. Les protocoles de cette couche segmentent et rassemblent les données envoyées par les applications de couche supérieure en un flux de données identique, qui offre des services de transport de bout en bout.

Les deux principaux rôles de la couche transport sont donc le contrôle de flux et la fiabilité. Elle définit une connectivité de bout en bout entre les applications hôtes. Voici quelques services de transport de base:

- Segmentation des données d'application de couche supérieure.
- Établissement d'une connexion de bout en bout.
- Transport des segments d'un hôte d'extrémité à un autre.
- Contrôle du flux assuré par les fenêtres glissantes.
- Fiabilité assurée par les numéros de séquence et les accusés de réception.

TCP/IP est une combinaison de deux protocoles distincts : IP et TCP. IP opère au niveau de la couche 3 du modèle OSI et est un protocole non orienté connexion offrant un acheminement au mieux (best-effort delivery) sur le réseau. TCP opère au niveau de la couche transport. C'est un service orienté connexion qui assure le contrôle du flux et la fiabilité. Combinés, ces deux protocoles offrent une gamme de services plus vaste. Ils constituent la base de la pile de protocoles TCP/IP, et c'est sur cette pile de protocoles que repose Internet.

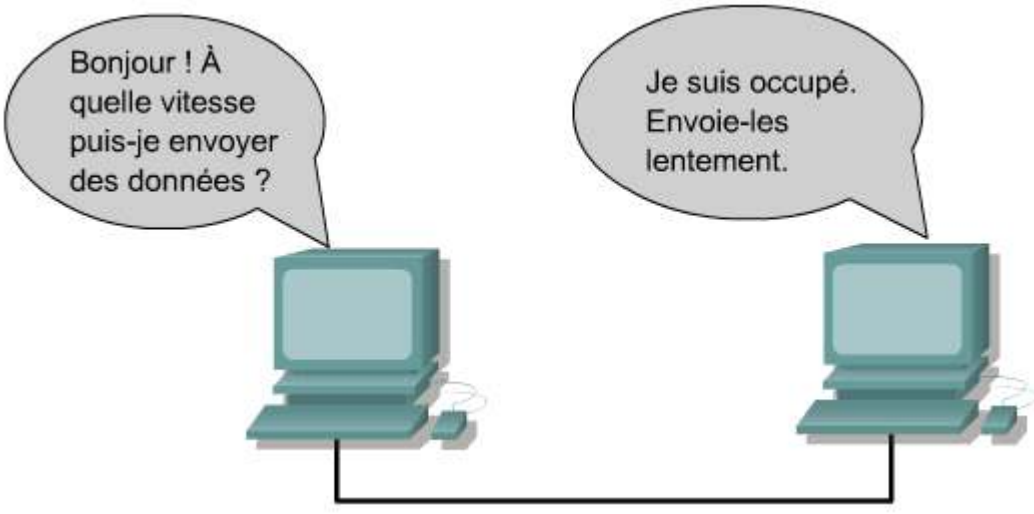
La page suivante explique le contrôle du flux de données par la couche transport.

11.1 Couche transport TCP/IP

11.1.2 Contrôle de flux

Cette page décrit le contrôle de flux par la couche transport.

Lorsque la couche transport envoie des segments de données, elle cherche à s'assurer que les données ne se perdent pas. Des données peuvent en effet être perdues si un hôte n'est pas capable de les traiter suffisamment vite au fur et à mesure qu'il les reçoit. Il est alors obligé de les rejeter. Le contrôle de flux permet d'éviter le dépassement de capacité des mémoires tampons d'un hôte de destination. Pour ce faire, TCP met en relation les hôtes source et de destination qui conviennent alors d'un taux de transfert des données acceptable. 1



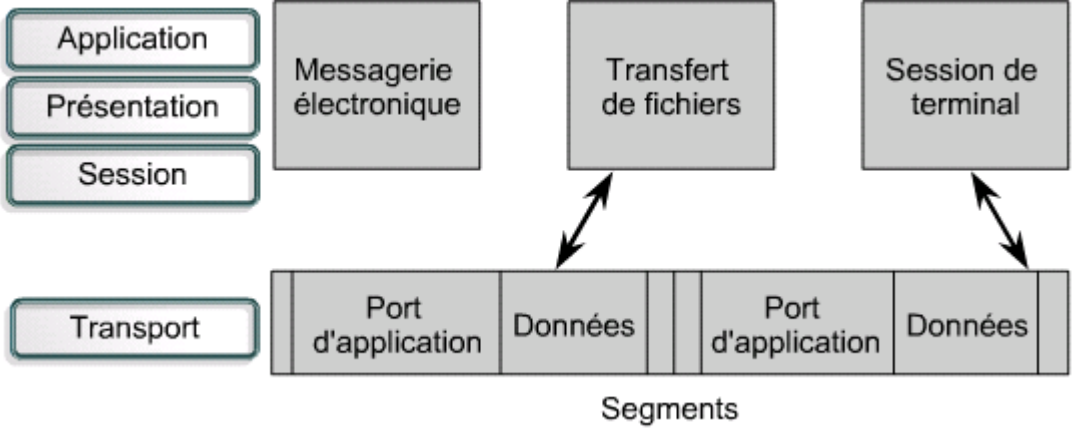
La page suivante traite des connexions de transport des données.

11.1 Couche transport TCP/IP

11.1.3 Établissement, maintenance et fermeture de session

Cette page présente le transport à proprement parler et son principe de fonctionnement reposant sur les segments.

Les applications envoient des segments de données suivant la méthode du premier arrivé, premier servi. Les segments les premiers arrivés sont pris en charge les premiers. Ils peuvent être acheminés vers une même destination ou vers des destinations différentes. Dans le modèle de référence OSI, plusieurs applications peuvent partager la même connexion de transport. On parle alors de multiplexage des conversations de couche supérieure. [1]

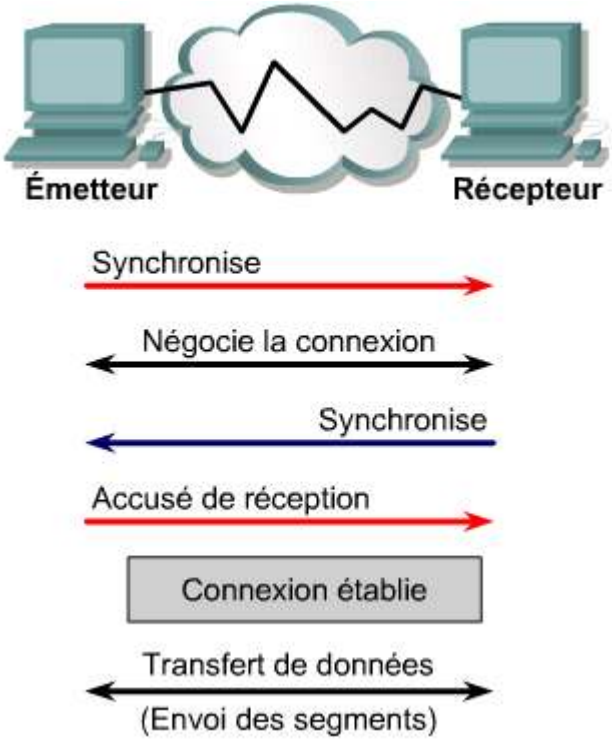


Plusieurs conversations simultanées de couche supérieure peuvent être multiplexées sur une seule connexion.

Un des rôles de la couche transport est d'établir une session orientée connexion entre des unités identiques de la couche application. Pour que le transfert de données puisse débuter, les applications source et de destination doivent informer leur système d'exploitation qu'une connexion va être initiée. Un des nœuds initie la connexion qui doit obligatoirement être acceptée par l'autre. Les modules logiciels de protocole des deux systèmes d'exploitation communiquent en envoyant des messages sur le réseau pour vérifier si le transfert est autorisé et si les deux ordinateurs sont prêts.

La connexion est établie et le transfert des données peut commencer après synchronisation. Pendant le transfert, les deux ordinateurs continuent de communiquer au moyen de leur logiciel de protocole pour vérifier si les données sont bien reçues.

La figure 2



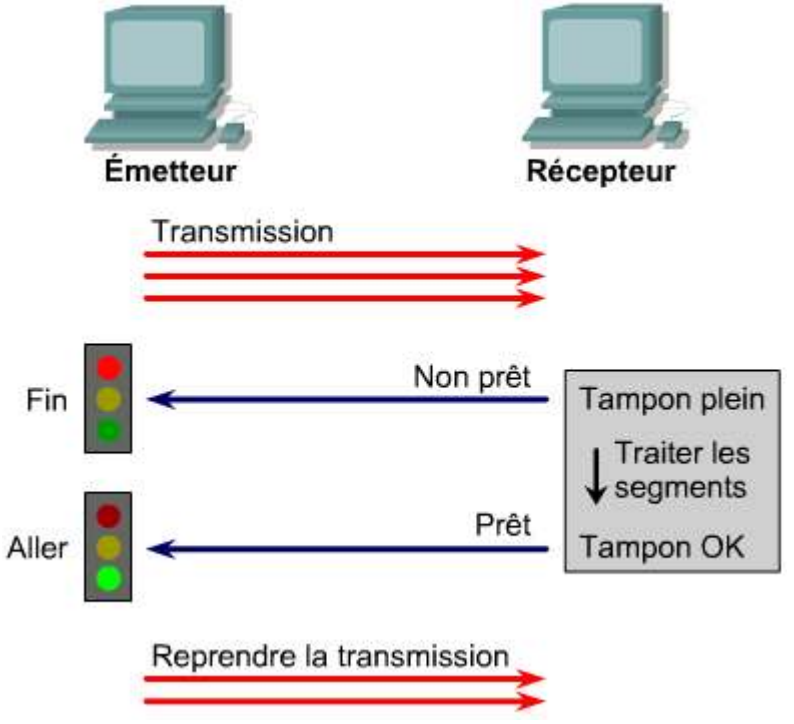
montre une connexion type établie entre deux systèmes. La première étape du protocole d'échange bidirectionnel demande la synchronisation. Le deuxième échange accuse réception de la demande de synchronisation initiale et synchronise les paramètres de connexion dans la direction opposée. Le troisième segment d'échange est un accusé de réception indiquant à la destination que la connexion peut être établie des deux côtés. Une fois la connexion établie, le transfert des données commence.

Une congestion peut se produire lors de deux situations:

- Lorsqu'un ordinateur génère un trafic dont le débit est plus rapide que la vitesse de transfert du réseau.
- Lorsque plusieurs ordinateurs doivent envoyer simultanément des datagrammes à une même destination (celle-ci peut alors devenir encombrée, même si le problème ne provient pas d'une seule source).

Lorsque des datagrammes arrivent trop rapidement et que l'ordinateur ou la passerelle ne peut les traiter, ils sont stockés temporairement en mémoire. Si le trafic continue, la mémoire de l'hôte ou de la passerelle finit par être saturée et les datagrammes qui arrivent doivent être abandonnés.

Pour éviter la perte des données, le processus TCP de l'hôte récepteur envoie un indicateur «non prêt» à l'émetteur, afin que ce dernier arrête de transmettre. Lorsque le récepteur peut accepter de nouvelles données, il envoie l'indicateur de transport «prêt» à l'émetteur qui reprend alors la transmission des segments. 3



Une fois le transfert des données terminé, l'hôte source envoie un signal indiquant la fin de la transmission. L'hôte de destination accuse réception et la connexion se termine.

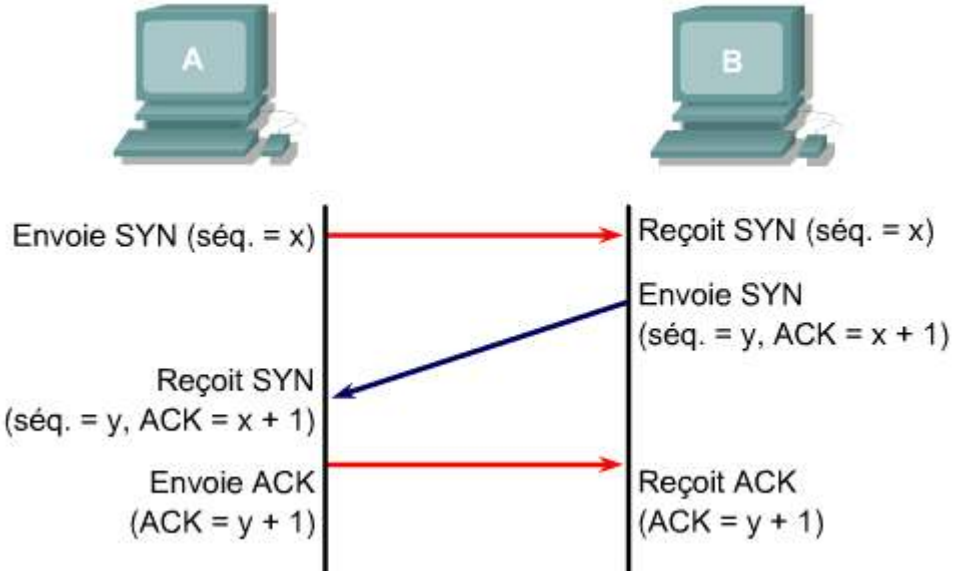
La page suivante définit les échanges en trois étapes.

11.1 Couche transport TCP/IP
11.1.4 Échange en trois étapes

Cette page explique l'utilisation des échanges en trois étapes par TCP pour la transmission des données.

Le protocole TCP est orienté connexion. Une connexion doit par conséquent être établie avant le début du transfert des données. Pour établir cette connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (ISN – Initial Sequence Number). La synchronisation s'effectue par le biais d'un échange de segments transportant un bit de contrôle SYN (synchroniser) et les numéros de séquence initiaux. Cette méthode nécessite une opération pour sélectionner les numéros de séquence initiaux et un protocole d'échange bidirectionnel pour les échanger.

La synchronisation nécessite que chaque hôte envoie son propre numéro de séquence initial (ISN) et reçoive une confirmation de cet échange par un accusé de réception (ACK) envoyé par l'autre hôte. Chaque hôte doit donc recevoir le ISN envoyé par l'autre hôte et répondre en envoyant un message ACK. La séquence est la suivante: 1



1. L'hôte émetteur (A) initie une connexion en envoyant un paquet SYN à l'hôte récepteur (B) indiquant que son numéro de séquence initial ISN = X:

   A —> B SYN, séq. de A = X

2. B reçoit le paquet, enregistre que la séq. de A = X, répond par un accusé de réception de X + 1 et indique que son numéro de séquence ISN = Y. L'accusé X + 1 signifie que l'hôte B a reçu tous les octets jusqu'à X inclus et qu'il attend l'arrivée de X + 1:

   B —> A ACK, séq. de A = X, SYN séq. de B = Y, ACK = X + 1

3. L'hôte A reçoit le paquet de B, apprend que la séquence de B est Y et répond par un accusé de Y + 1, qui met fin au processus de connexion:

   A —> B ACK, séq. de B = Y, ACK = Y + 1

Cet échange est un échange en trois étapes.

Il est essentiel car les numéros de séquence ne reposent pas sur une horloge universelle sur le réseau et les méthodes utilisées par les protocoles TCP pour choisir les numéros de séquence initiaux peuvent différer. Le récepteur du premier SYN ne peut savoir si le segment a été différé à moins de conserver une trace du dernier numéro de séquence utilisé dans la connexion. Sans cette information, il doit demander à l'émetteur de vérifier le SYN.

La page suivante présente le concept de fenêtrage.

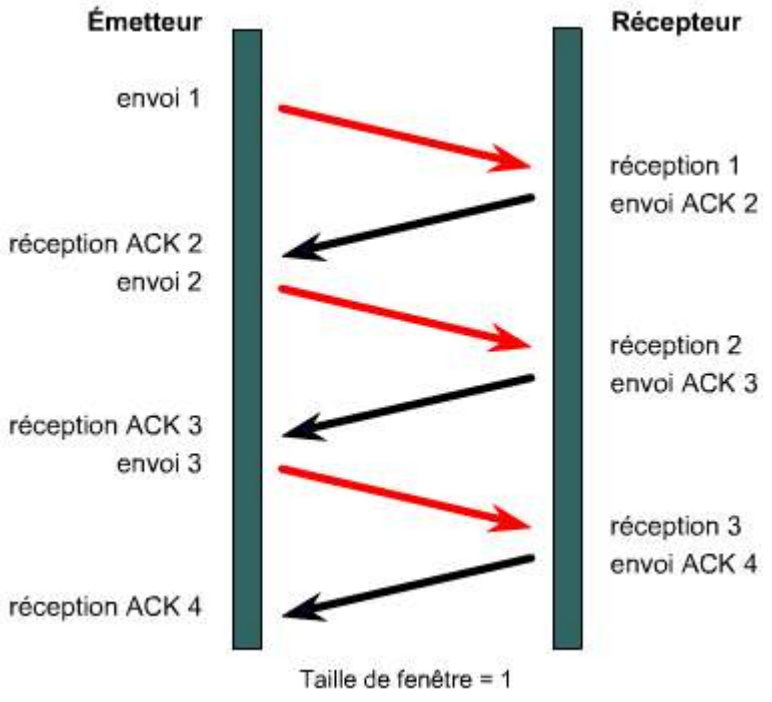
11.1 Couche transport TCP/IP

11.1.5 Fenêtrage

Cette page explique l'utilisation des fenêtres dans la transmission des données.

Pour qu'un transfert de données soit orienté connexion et fiable, les paquets de données doivent être délivrés au destinataire dans le même ordre que celui dans lequel ils ont été transmis. Le protocole échoue si des paquets de

données sont perdus, endommagés, dupliqués ou reçus dans un ordre différent. Une solution simple consiste, pour le destinataire, à accuser réception de chacun des paquets avant que le paquet suivant ne lui soit envoyé.



1

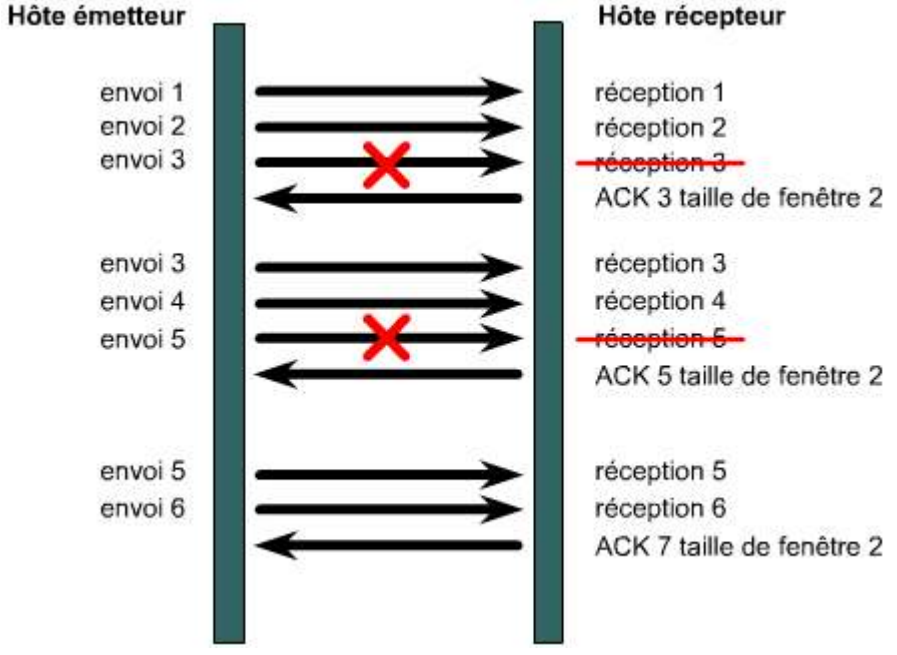
Toutefois, si l'émetteur devait attendre un accusé de réception après l'envoi de chaque paquet, le débit serait particulièrement lent. C'est pourquoi la plupart des protocoles orientés connexion fiables permettent l'envoi de plusieurs paquets avant qu'un accusé ACK ne soit effectivement reçu. L'émetteur utilise l'intervalle de temps qui s'écoule entre le moment où il envoie un paquet et celui où il traite l'accusé de réception pour transmettre d'autres données. Le nombre de paquets de données pouvant ainsi être transmis avant réception d'un accusé de réception est connu sous le nom de taille de fenêtre ou fenêtre.

TCP utilise des accusés de réception prévisionnels. Cela signifie que le numéro de l'accusé indique le paquet suivant attendu.

Le fenêtrage fait référence au fait que la taille de la fenêtre est négociée de manière dynamique pendant la session TCP. Il constitue un mécanisme de contrôle de flux. Après qu'une certaine quantité de données a été transmise, la machine source doit recevoir un accusé de l'hôte de destination. Ce dernier signale une taille de fenêtre à l'hôte source. Cette fenêtre indique le nombre de paquets que l'hôte de destination est prêt à recevoir, le premier d'entre eux étant l'accusé de réception.

Si la taille de fenêtre est de trois, l'hôte source peut envoyer trois octets à l'unité de destination avant d'attendre l'accusé de réception. Lorsque l'hôte de destination reçoit les trois octets, il envoie un accusé de réception à la source qui peut alors envoyer trois autres octets. Si l'unité de destination ne reçoit pas ces trois octets, parce que ses mémoires tampons sont saturées, elle n'envoie pas d'accusé de réception. L'hôte source sait alors qu'il doit retransmettre les octets à un débit de transmission inférieur.

Dans la figure 2,



l'émetteur envoie trois paquets avant d'attendre l'accusé de réception. Si le récepteur ne peut en traiter que deux, la fenêtre abandonne le troisième paquet, indique que le paquet 3 sera le paquet suivant, puis spécifie une nouvelle fenêtre de deux. L'émetteur envoie les deux autres paquets, mais continue d'indiquer une taille de fenêtre de trois. Il attend donc toujours que le récepteur lui envoie un accusé de réception tous les trois paquets. Le récepteur répond en demandant le paquet cinq et indique de nouveau une taille de fenêtre de deux.

La page suivante décrit le mécanisme d'accusés de réception.

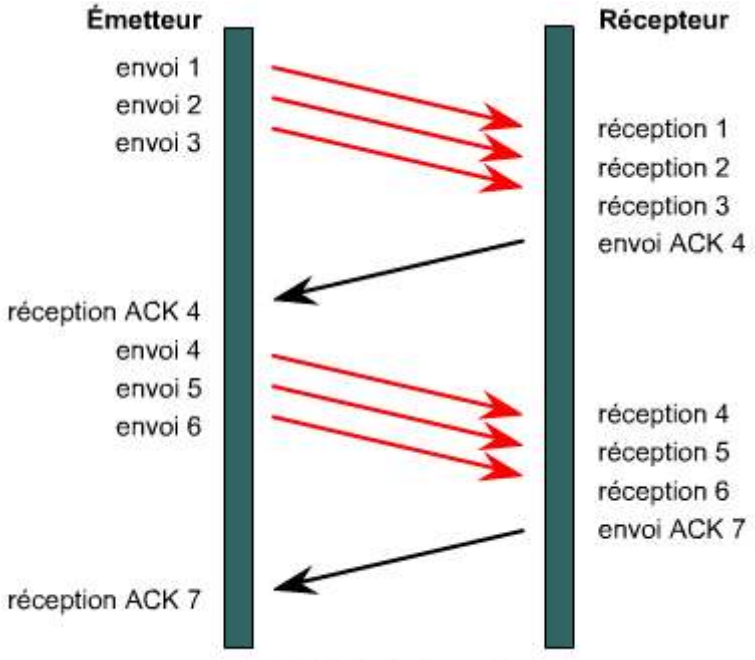
11.1 Couche transport TCP/IP

11.1.6 Accusé de réception

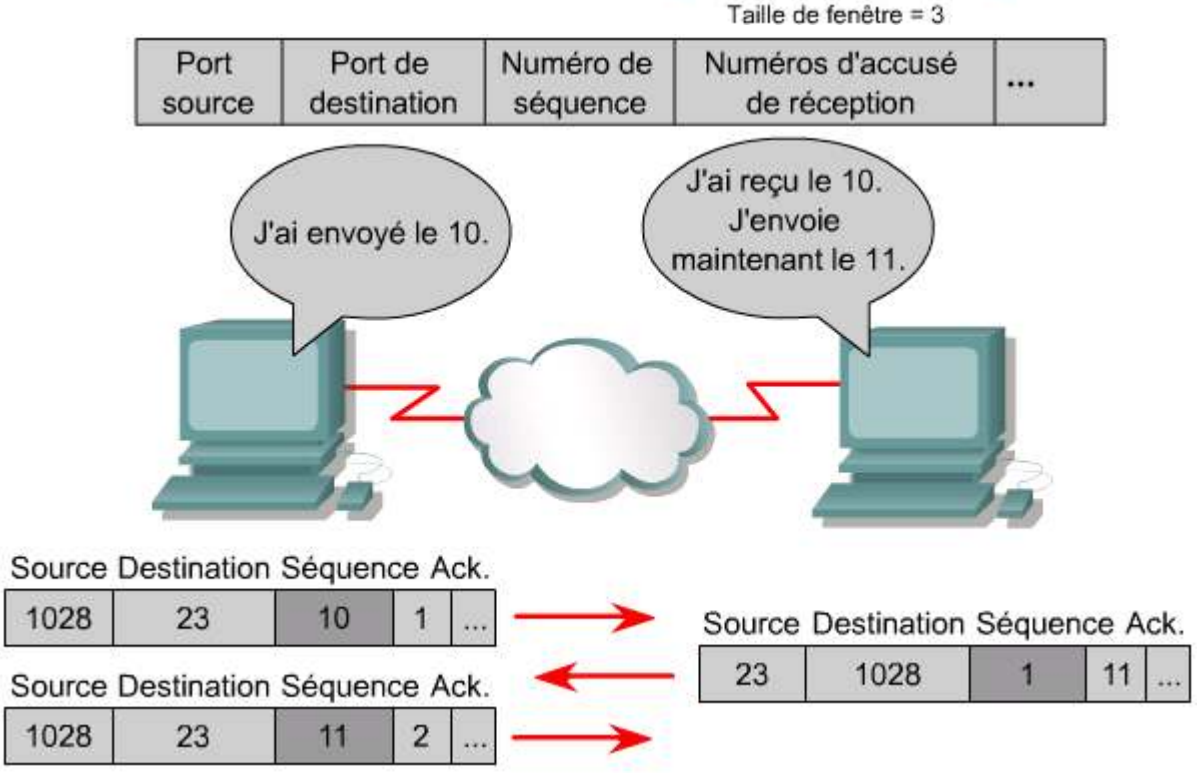
Cette page explique le mécanisme d'accusés de réception et le séquençage des segments.

Une transmission fiable garantit qu'un flux de données envoyé depuis un ordinateur sera acheminé via une liaison de données vers un autre ordinateur, sans duplication ni perte des données. Un accusé de réception positif avec retransmission est une technique qui garantit cette fiabilité. Ce type d'accusé nécessite que le destinataire communique avec la source en lui envoyant un message pour accuser réception des données. L'émetteur conserve un enregistrement de chaque paquet de données, ou segment TCP, qu'il envoie, puis attend un accusé de réception. De plus, un décompte est entamé lorsque l'émetteur envoie un segment et ce dernier est retransmis si le délai arrive à expiration avant l'arrivée de l'accusé de réception.

La figure 1 montre un émetteur transmettant les paquets 1, 2 et 3. Le destinataire accuse réception des paquets en demandant le paquet 4. À réception de l'accusé, l'émetteur envoie les paquets 4, 5 et 6. Si le paquet 5 n'arrive pas à destination, le récepteur demande sa retransmission. L'émetteur envoie alors le paquet 5, puis reçoit un accusé de réception lui demandant le paquet 7.



Le protocole TCP assure le séquençage des segments grâce à des accusés de réception vers l'avant. Chaque segment est numéroté avant la transmission. 2


Taille de fenêtre = 3
Port source
Port de destination
Numéro de séquence
Numéros d'accusé de réception
...
J'ai envoyé le 10.
J'ai reçu le 10. J'envoie maintenant le 11.
Source Destination Séquence Ack.
1028 23 10 1 ...
Source Destination Séquence Ack.
23 1028 1 11 ...
Source Destination Séquence Ack.
1028 23 11 2 ...

Arrivés à destination, ces segments sont rassemblés en un message complet par le protocole TCP. Si un numéro de séquence est absent de la série, le segment correspondant est retransmis. Les segments qui ne font pas l'objet d'un accusé de réception dans un délai donné sont retransmis.

La page suivante décrit le protocole TCP plus en détail.

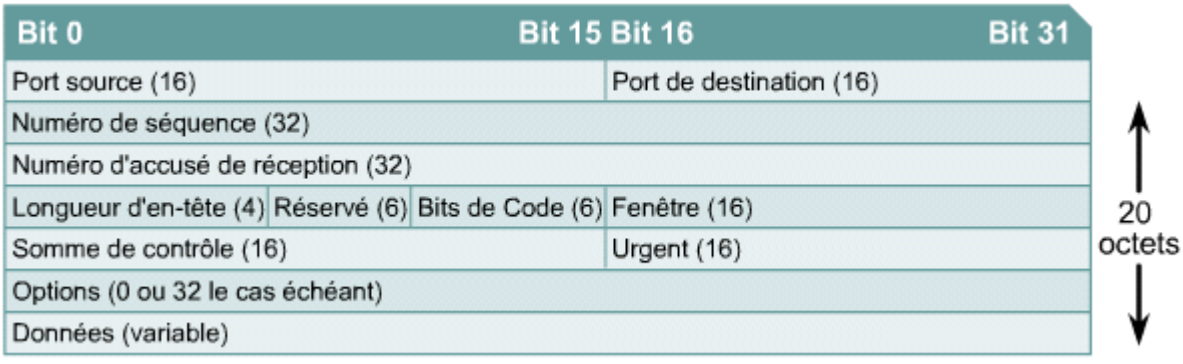
Cette page présente les protocoles utilisant TCP et les champs d'un segment TCP.

TCP est un protocole orienté connexion de la couche transport, qui assure une transmission fiable des données en full duplex. TCP fait partie de la pile de protocoles TCP/IP. Dans un environnement orienté connexion, une connexion est établie entre les deux extrémités avant que le transfert des informations ne commence. TCP découpe les messages en segments, les rassemble à l'arrivée et renvoie toute donnée non reçue. Il assure un circuit virtuel entre les applications utilisateur.

Les protocoles utilisant TCP sont les suivants:

- FTP
- HTTP
- SMTP
- Telnet

Voici la description des champs contenus dans le segment TCP: 1



- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Numéro de séquence:** numéro utilisé pour garantir une livraison des données dans l'ordre approprié.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle, telles que l'ouverture et la fermeture d'une session.
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** une des options actuellement disponibles est la taille maximale d'un segment TCP (MSS – Maximum Segment Size).
- **Données:** données de protocole de couche supérieure.

La page suivante présente le protocole UDP.

11.1 Couche transport TCP/IP

11.1.8 Protocole UDP (User Datagram Protocol)

Cette page porte sur le protocole UDP. UDP est un protocole de transport non orienté connexion de la pile de protocoles TCP/IP.

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison. Il repose entièrement sur les protocoles de couche supérieure pour le contrôle des erreurs et la retransmission des données.

UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.

Les protocoles utilisant UDP sont les suivants:

- TFTP
- SNMP
- DHCP
- DNS

Voici la description des champs contenus dans le segment UDP: 1



- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Données:** données de protocole de couche supérieure.

La page suivante aborde les numéros de port utilisés par les protocoles TCP et UDP.

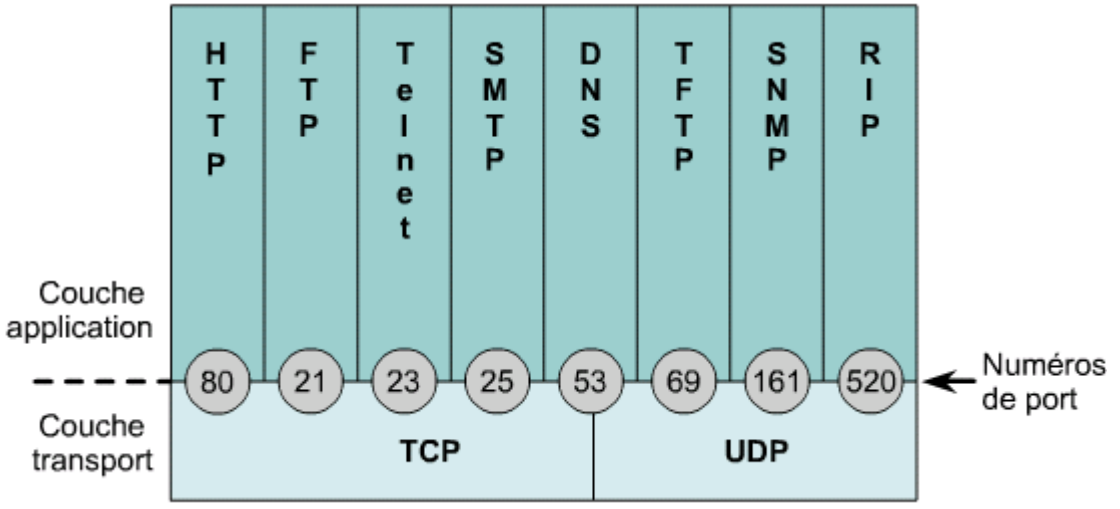
11.1 Couche transport TCP/IP

11.1.9 Numéros de port TCP et UDP

Cette page étudie les numéros de port.

Les protocoles TCP et UDP utilisent des numéros de port pour transmettre les informations aux couches supérieures. Ces numéros servent à distinguer les différentes conversations qui circulent simultanément sur le réseau.

Les développeurs d'applications ont convenu d'utiliser les numéros de port reconnus émis par l'IANA (*Internet Assigned Numbers Authority*). 1



Toute conversation destinée à l'application FTP fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie données et le port 21 pour le contrôle. Les conversations qui n'impliquent pas d'application utilisant un numéro de port reconnu se voient attribuer des numéros de manière aléatoire sélectionnés dans une plage spécifique supérieure à 1023. Certains ports sont réservés aux protocoles TCP et UDP, bien que les applications ne soient pas forcément conçues pour les prendre en charge. 2

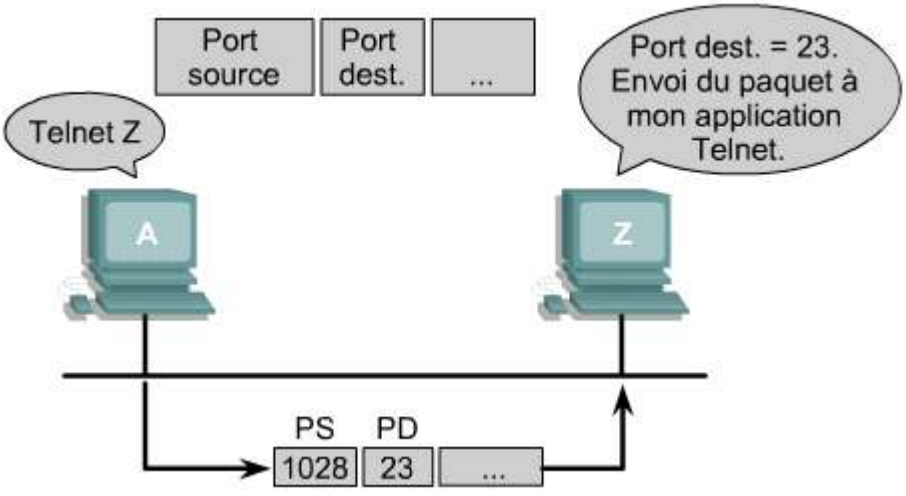
Decimal	Keyword	Description
0		Réservé
1-4		Non attribué
5	RJE	Protocole RJE (Soumission de travaux à distance)
7	ECHO	Écho
9	DISCARD	Élimination
11	USERS	Utilisateurs actifs
13	DAYTIME	Heure du jour
15	NETSTAT	Qui est actif ou NETSTAT
17	QUOTE	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-DATA	Protocole FTP (données)
21	FTP	Protocole FTP
23	TELNET	Connexion en mode terminal
25	SMTP	Protocole SMTP (Simple Mail Transfer Protocol)
37	TIME	Heure du jour
39	RLP	Protocole RLP (Resource Location Protocol)
42	NAMESERVER	Serveur de noms d'hôte

43	NICNAME	Protocole Who Is
53	DOMAIN	Serveur de noms de domaine
67	BOOTPS	Serveur de protocole Bootstrap
68	BOOTPC	Client de protocole Bootstrap
69	TFTP	Protocole TFTP (Trivial File Transfer Protocol)
75		Tout service de sortie privé
77		Tout service RJE privé
79	FINGER	Finger
80	HTTP	Protocole HTTP (HyperText Transfer Protocol)
95	SUPDUP	Protocole SUPDUP
101	HOSTNAME	Serveur de noms d'hôte NIC
102	ISO-TSAP	ISO-TSAP
113	AUTH	Service d'authentification
117	UUCP-PATH	Service de chemin UUCP
123	NTP	Protocole NTP (Network Time Protocol)
137	NetBIOS	Service de noms
139	NetBIOS	Service de datagramme
143	IMAP	Protocole IMAP (Interim Mail Access Protocol)
150	NetBIOS	Service de session
156	SQL	Serveur SQL
161	SNMP	Protocole SNMP (Simple Network Management Protocol)
179	BGP	Protocole BGP (Border Gateway Protocol)
190	GACP	Protocole GACP (Gateway Access Control Protocol)
194	IRC	IRC (Internet Relay Chat)
197	DLS	Directory Location Service
224-241		Non attribué
242-255		Non attribué

Les plages attribuées aux numéros de port sont les suivantes:

- Les numéros inférieurs à 1024 sont considérés comme des numéros de port reconnus.
- Les numéros supérieurs à 1023 sont des numéros attribués de manière dynamique.
- Les numéros de port enregistrés sont destinés à des applications spécifiques d'un fournisseur. La plupart se situent au-delà de 1024.

Les systèmes d'extrémité utilisent les numéros de port pour sélectionner l'application appropriée. L'hôte source attribue dynamiquement les numéros de port source. Ils sont toujours supérieurs à 1023. 3



Cette page termine la leçon. La leçon suivante porte sur la couche application. La première page constitue une introduction.

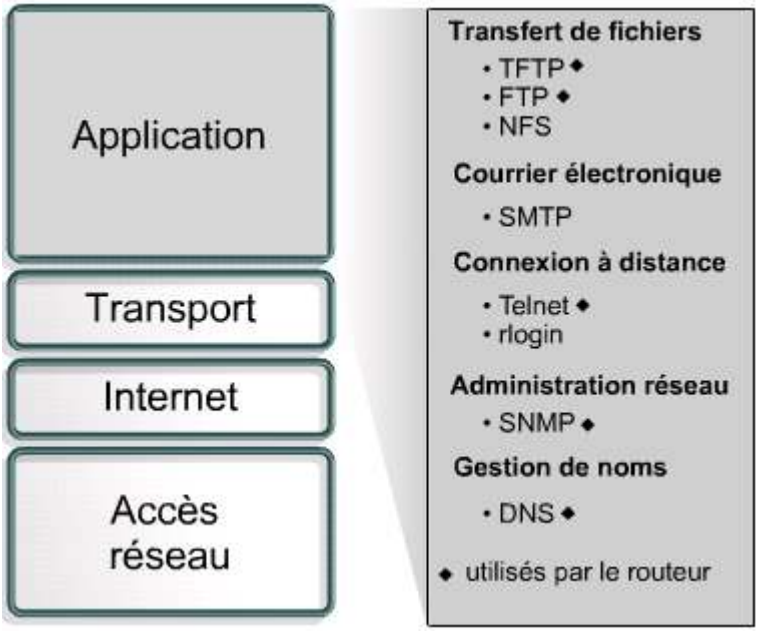
11.2 La couche application

11.2.1 Introduction à la couche application du modèle TCP/IP

Cette page présente quelques protocoles de la couche application TCP/IP.

Les couches session, présentation et application du modèle OSI sont regroupées dans la couche application du modèle TCP/IP. Cela signifie que la représentation, le code et le contrôle du dialogue sont traités au niveau de la couche application TCP/IP. Cette structure permet de garantir un maximum de flexibilité dans la couche application du modèle TCP/IP pour les développeurs d'applications.

Les protocoles TCP/IP qui prennent en charge le transfert des fichiers, la messagerie et la connexion à distance sont probablement les protocoles que connaissent le mieux les utilisateurs d'Internet. [1]



Ils comprennent les applications suivantes:

- DNS
- FTP
- HTTP
- SMTP
- SNMP
- Telnet

La page suivante aborde le système DNS.

11.2 La couche application
11.2.2 DNS

Cette page porte sur le système DNS.

Internet repose sur un système d'adressage hiérarchique qui permet un routage basé sur des classes d'adresses plutôt que sur des adresses individuelles. Le problème pour l'utilisateur est de faire correspondre l'adresse désirée avec le site Internet. Il est difficile de retenir l'adresse IP d'un site, car l'adresse numérique n'a aucun rapport apparent avec le contenu du site. Imaginez la difficulté que cela représenterait de mémoriser les adresses IP de dizaines, de centaines, voire de milliers de sites Web.

Afin de pouvoir créer un lien entre le contenu d'un site et son adresse, un système de noms de domaine a été établi. Le système de noms de domaine (DNS) est utilisé sur Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement. Un domaine est un groupe d'ordinateurs associés en fonction de leur proximité géographique ou du type d'informations qu'ils contiennent. Un nom de domaine est une chaîne de caractères, de nombres, ou les deux. Il s'agit généralement d'un nom ou d'une abréviation qui est associé à l'adresse numérique d'un site Internet. Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment:

.us – États-Unis
.fr – France

Il existe aussi des noms génériques, notamment:

.edu – sites éducatifs
.com – sites commerciaux
.gov – sites gouvernementaux
.org – sites d'organisations à but non lucratif
.net – service de réseau

Reportez-vous à la figure 1

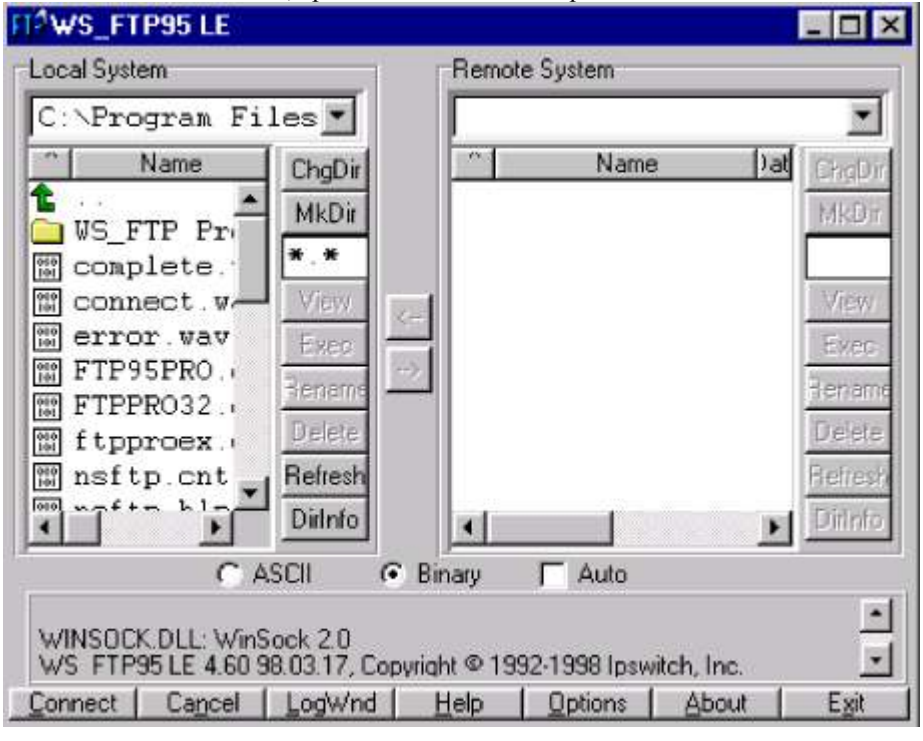
Domaines génériques internationaux	
COM -	Ce domaine est réservé aux entités commerciales, c'est-à-dire aux entreprises. Il a pris beaucoup d'ampleur et certains s'inquiètent de la charge administrative et des performances du système si le rythme de croissance actuel se maintient. On évalue la possibilité de subdiviser le domaine COM et de permettre l'enregistrement futur des entreprises dans ces sous-domaines.
EDU -	Ce domaine a été conçu à l'origine pour tous les établissements d'enseignement. Un grand nombre de consortiums éducatifs, d'écoles, d'établissements d'enseignement supérieur, d'universités et de services éducatifs se sont enregistrés dans ce domaine. Plus récemment, il a été décidé de limiter les enregistrements futurs aux universités et aux établissements d'enseignement supérieur sur 4 ans. Les écoles et les établissements d'enseignement supérieur sur 2 ans seront enregistrés dans les domaines de pays (voir le domaine US ci-dessous et les subdivisions de la maternelle à la 12e année et CC plus particulièrement).
NET -	Ce domaine est réservé aux ordinateurs des fournisseurs de réseau : les ordinateurs du NIC (Network Information Center) et du centre d'exploitation du réseau NOC (Network Operation Center), les ordinateurs administratifs et les ordinateurs des nœuds réseau. Les clients du fournisseur de réseau ont leur propre nom de domaine (pas dans le domaine de niveau supérieur NET).
ORG -	Ce domaine de niveau supérieur est réservé aux organisations qui n'entrent dans aucune autre catégorie. Certaines organisations non gouvernementales peuvent être classées dans cette catégorie.
INT -	Ce domaine est destiné aux organismes établis par des traités internationaux ou aux bases de données internationales.
Domaines génériques spécifiques des États-Unis	
GOV -	Ce domaine était à l'origine destiné à tous les bureaux ou agences gouvernementaux. Plus récemment, il a été décidé de n'y enregistrer que les agences du gouvernement fédéral américain. Les agences locales et fédérales sont inscrites sous le domaine du pays.
MIL -	Ce domaine est utilisé par l'armée américaine.
Exemple de domaine de pays	
US -	En tant qu'exemple de domaine de pays, le domaine US permet l'enregistrement de toutes sortes d'entités aux États-Unis, en fonction de la géographie politique, c'est-à-dire selon une hiérarchie <nom-entité>.<localité>. <code état>. US. Par exemple, IBM.Armonk.NY.US. En outre, des branches du domaine US ont été prévues au sein de chaque État pour les écoles maternelles, primaires et secondaires, les collèges publics (CC), les écoles techniques (TEC), les agences d'état (STATE), les conseils de gouvernement (COG), les bibliothèques (LIB), les musées (MUS) et plusieurs autres types génériques

pour une explication détaillée de ces domaines.

La page suivante aborde les protocoles FTP et TFTP.

Cette page décrit les fonctions des protocoles FTP et TFTP.

FTP est un service orienté connexion fiable qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. L'objectif principal du protocole FTP est d'échanger des fichiers dans les deux sens (importation et exportation) entre un ordinateur serveur et des ordinateurs clients. Lorsque vous importez des fichiers à partir d'un serveur, FTP établit d'abord une connexion de contrôle entre le client et le serveur. Puis une seconde connexion permet de transférer les données d'un ordinateur à l'autre. Le transfert des données peut se faire en mode ASCII ou binaire. Ces modes déterminent le codage des fichiers de données qui, dans le modèle OSI, constitue une tâche de la couche présentation. Une fois le fichier transféré, la connexion de données est automatiquement interrompue. La commande de liaison est fermée dès que l'utilisateur met fin à la session en se déconnectant, après avoir terminé de copier et de transférer ses fichiers. 1



TFTP est un service non orienté connexion qui se sert du protocole UDP (*User Datagram Protocol*). Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Ce protocole, conçu pour être léger et facile à mettre en œuvre, est dépourvu de la plupart des fonctionnalités de FTP. Il peut lire ou écrire des fichiers vers ou depuis un serveur distant, mais il ne permet pas d'afficher le contenu des répertoires ni d'assurer l'authentification des utilisateurs. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP. Son fonctionnement est par ailleurs fiable dans un environnement stable.

La page suivante aborde le protocole HTTP.

Cette page présente les fonctionnalités du protocole HTTP.

Le protocole HTTP (*Hypertext Transfer Protocol*) est le support du Web, la partie la plus utilisée d'Internet et celle qui connaît la plus forte croissance. L'expansion phénoménale du Web s'explique principalement par la facilité avec laquelle il permet d'accéder aux informations. Un navigateur Web est une application de type client-serveur, c'est-à-dire qu'il requiert un composant client et un composant serveur pour pouvoir fonctionner. Il présente des pages Web contenant des données multimédia : texte, graphique, son et vidéo. Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier. Outre le contenu, le langage HTML spécifie la disposition du texte, des fichiers et des objets qui sont transférés depuis le serveur Web jusqu'au navigateur Web.

Les liens hypertexte (ou hyperliens) facilitent la navigation sur le Web. Il peut s'agir d'un objet, d'un mot, d'une phrase ou d'une image sur une page Web. Lorsque vous cliquez sur ce lien, une nouvelle page Web est affichée dans le navigateur. La page Web contient une adresse URL (*Uniform Resource Locator*) qui est souvent cachée dans sa description HTML.

Dans l'URL http://www.cisco.com/edu/, la partie «http://» indique au navigateur le protocole à utiliser. La seconde partie, «www», indique le nom de l'hôte ou le nom d'un ordinateur précis doté d'une adresse IP spécifique. Enfin, le suffixe « /edu/ » précise l'emplacement exact du dossier sur le serveur qui contient la page Web. 1

http://	www.	cisco.com	/edu/
Indique au navigateur le protocole à utiliser.	Indique le nom de l'hôte ou le nom d'un ordinateur précis.	Représente l'entité de domaine du site Web.	Spécifie le répertoire dans lequel la page Web est située sur le serveur. Ainsi, quand aucun nom n'est spécifié, le navigateur charge la page par défaut identifiée par le serveur.

Cette figure indique les parties d'une adresse URL (Uniform Resource Locator) standard.

Un navigateur Web s'ouvre généralement sur une page de démarrage ou page d'accueil. L'adresse URL a été enregistrée dans les données de configuration du navigateur et peut être modifiée quand bon vous semble. Dans cette page d'accueil, vous pouvez soit cliquer sur un hyperlien, soit taper une adresse URL dans la barre d'adresse du navigateur. Le navigateur Web examine alors le protocole pour savoir s'il a besoin d'ouvrir un autre programme, puis détermine l'adresse IP du serveur Web à l'aide du système DNS. Ensuite, les couches transport, réseau, liaison de données et physique établissent une session avec le serveur Web. Les données transférées vers le serveur HTTP contiennent le nom du dossier où est stockée la page Web. Les données peuvent également contenir le nom de fichier d'une page HTML. En l'absence de nom, le nom par défaut indiqué dans la configuration du serveur est utilisé.

Le serveur répond à la demande en transmettant au client Web tous les fichiers texte, audio, vidéo et graphique indiqués dans la page HTML. Le navigateur client rassemble tous ces fichiers pour créer une image de la page Web et met fin à la session. Si vous cliquez sur une autre page située sur le même serveur, ou sur un serveur différent, la procédure reprend depuis le début.

Les étudiants peuvent effectuer le TP pour se familiariser avec les protocoles TCP et HTTP.

La page suivante présente le protocole utilisé dans l'envoi des messages électroniques.

Activité de TP

Exercice: Protocol Inspector, TCP et HTTP

Ce TP a pour objet l'utilisation du logiciel Protocol Inspector, ou tout autre logiciel équivalent, pour afficher les opérations TCP (*Transmission Control Protocol*) dynamiques. L'opération qui nous intéresse plus spécifiquement est HTTP lors de l'accès aux pages Web.

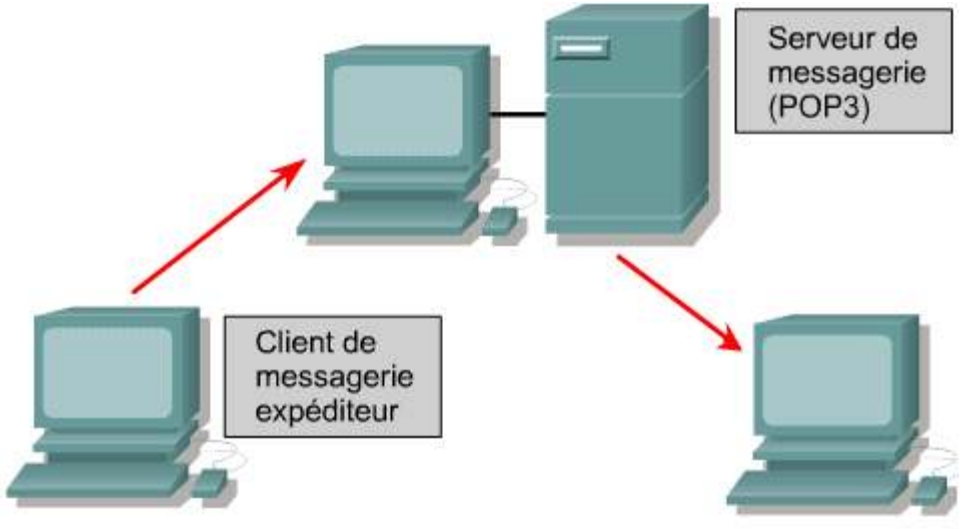
11.2 La couche application

11.2.5 SMTP

Cette page présente les fonctionnalités du protocole SMTP.

Les serveurs de messagerie communiquent entre eux à l'aide du protocole SMTP (*Simple Mail Transfer Protocol*) pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages au format ASCII à l'aide de TCP.

Lorsqu'un serveur de messagerie reçoit un message destiné à un client local, il le stocke jusqu'à ce que le client le récupère. 1



Lors de l'envoi d'un message électronique, celui-ci est d'abord envoyé au " bureau de poste " du destinataire. C'est là que le destinataire le récupère.

Les clients de messagerie peuvent récupérer leur courrier de plusieurs manières : soit ils se servent de programmes qui accèdent directement aux fichiers du serveur de messagerie, soit ils font appel à l'un des nombreux protocoles réseau. Les protocoles de client de messagerie les plus répandus sont POP3 et IMAP4, qui

utilisent tous deux TCP pour transporter les données. Bien que les clients de messagerie récupèrent le courrier via ces protocoles, ils utilisent pratiquement toujours le protocole SMTP pour l'envoi des messages. L'envoi et la réception de courrier faisant appel à deux protocoles différents, voire deux serveurs différents, les clients de messagerie peuvent très bien effectuer une tâche, mais pas l'autre. Il est par conséquent préférable de résoudre les problèmes d'envoi de courrier indépendamment des problèmes de réception.

Lorsque vous vérifiez la configuration d'un client de messagerie, assurez-vous que les paramètres SMTP et POP, ou IMAP, sont correctement configurés. Pour tester l'accès à un serveur de messagerie, établissez une connexion Telnet au port SMTP (25) ou au port POP3 (110). Le format de commande suivant est utilisé sur la ligne de commande Windows pour tester l'accès au service SMTP du serveur de messagerie à l'adresse IP 192.168.10.5:

```
C:\>telnet 192.168.10.5 25
```

Le protocole SMTP ne propose guère d'options de sécurité et ne nécessite aucune authentification. Généralement, les administrateurs n'autorisent que les hôtes appartenant à leur réseau à utiliser leur serveur SMTP pour l'envoi ou le transit de courrier. Cela dans le but d'éviter que des utilisateurs non autorisés n'utilisent leurs serveurs comme relais de messagerie.

La page suivante présente les fonctionnalités du protocole SNMP.

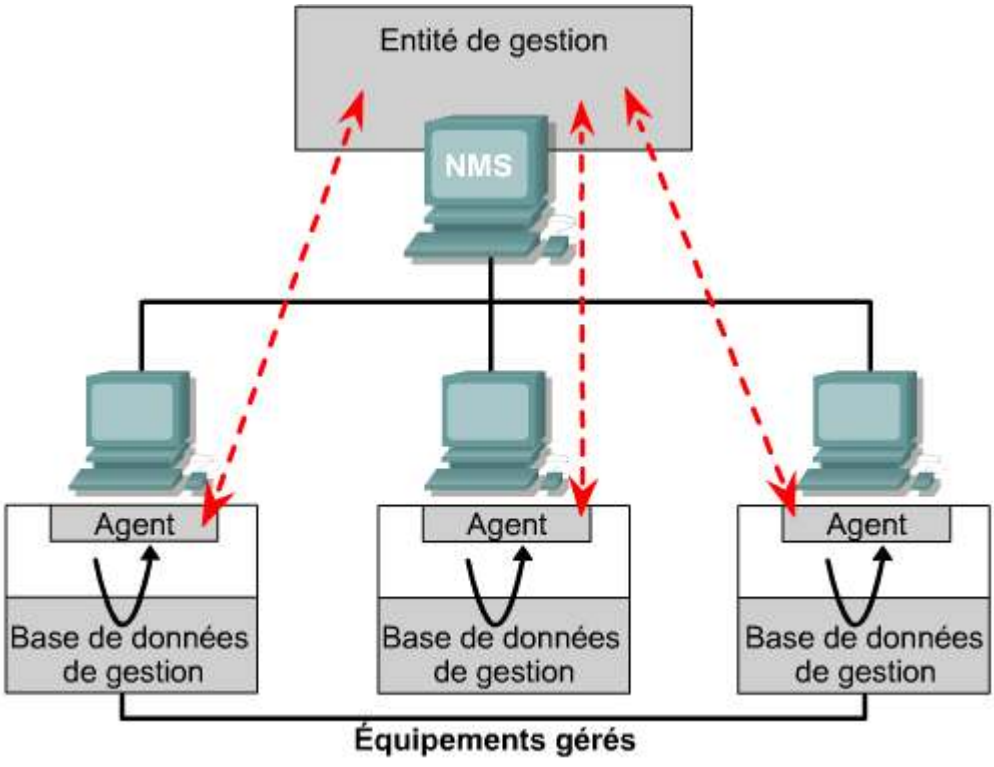
11.2.6	**SNMP**	

11.2.6	**SNMP**	

Cette page porte sur le protocole SNMP.

Le protocole SNMP (*Simple Network Management Protocol*) est un protocole de la couche application qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes, ainsi que d'anticiper la croissance du réseau. SNMP se sert du protocole UDP de la couche transport.

Un réseau géré à l'aide de SNMP comprend les trois principaux composants suivants: 1



- **Le système d'administration de réseaux *(NMS, Network Management System)*:** le composant NMS exécute les applications qui contrôlent et surveillent les unités gérées. Il fournit la quantité de ressources mémoire et de traitement requises pour la gestion du réseau. Tout réseau géré doit comprendre au moins un composant NMS.
- **Les unités gérées:** ces unités sont des nœuds du réseau contenant un agent SNMP et résidant sur un réseau géré. Elles collectent et stockent des informations de gestion qu'elles mettent à la disposition des composants NMS via SNMP. Ces unités gérées, parfois appelées éléments du réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.
- **Les agents:** les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.

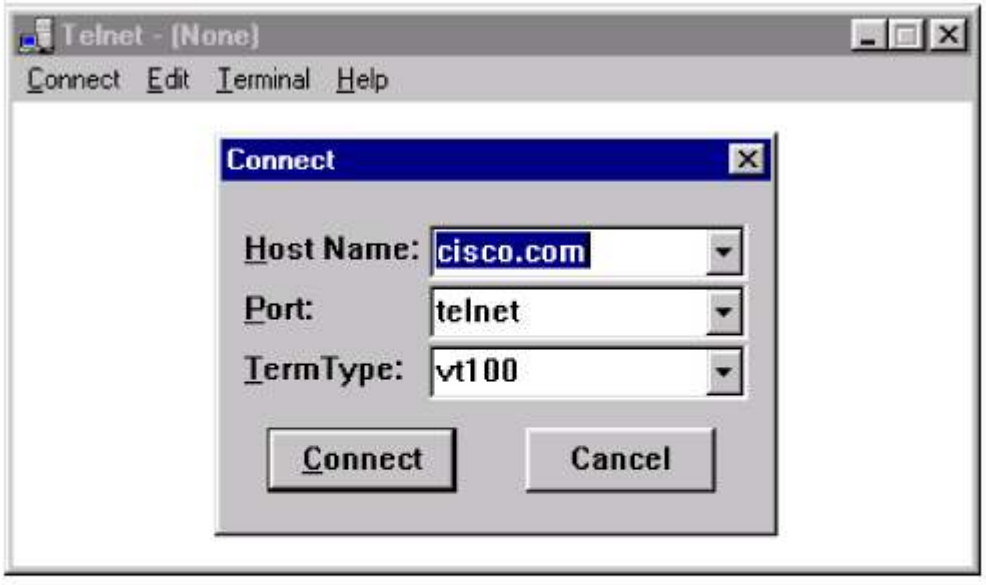
La page suivante présente le service Telnet.

11.2 La couche application

11.2.7 Service Telnet

Cette page explique les fonctionnalités de Telnet.

Le logiciel client Telnet permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande. Un client Telnet est qualifié d'hôte local. Le serveur Telnet, qui utilise un logiciel spécial appelé «démon», est considéré comme l'hôte distant. [1]



Une session Telnet démarre comme tout autre programme de communication, avec une adresse de connexion à un ordinateur hôte. Il peut s'agir d'une adresse IP, telle que 192.168.10.11, ou d'un nom de domaine.

Pour établir une connexion à partir d'un client Telnet, il convient de sélectionner une option de connexion. Une boîte de dialogue vous invite généralement à entrer un nom d'hôte et un type de terminal. Le nom d'hôte est l'adresse IP ou le nom DNS de l'ordinateur distant. Le type de terminal décrit le mode d'émulation de terminal qui doit être utilisé par le client Telnet. La connexion Telnet n'exige aucun traitement de la part de l'ordinateur émetteur qui se contente de transmettre à l'ordinateur distant les caractères tapés au clavier et d'afficher l'écran résultant sur le moniteur local. Les opérations de traitement et de stockage sont entièrement exécutées par l'ordinateur distant.

Telnet fonctionne au niveau de la couche application du modèle TCP/IP. Il opère donc au niveau des trois couches supérieures du modèle OSI. La couche application traite les commandes. La couche présentation gère le formatage, généralement ASCII. La couche session effectue la transmission. Dans le modèle TCP/IP, toutes ces fonctions sont regroupées dans la couche application.

Cette page termine la leçon. La page suivante récapitule les principaux points évoqués au cours de ce module.

Résumé

Cette page résume les sujets traités dans ce module.

Le rôle principal de la couche transport (couche 4 du modèle OSI) est de transporter et de contrôler le flux d'informations de la source à la destination, et ce de manière fiable et précise.

La couche transport multiplexe les données des applications de couche supérieure en un flux de paquets de données. Elle se sert de numéros de port (socket) pour identifier les différentes conversations et livrer les données aux applications appropriées.

Le protocole TCP (*Transmission Control Protocol*) est un protocole orienté connexion qui assure le contrôle du flux ainsi que la fiabilité. Il fait appel à un échange en trois étapes pour établir un circuit synchronisé entre les applications utilisateur. Chaque datagramme est numéroté avant la transmission. Au niveau de la station de

réception, le protocole TCP assemble le segment en un message complet. Si un numéro de séquence est absent de la série, le segment correspondant est retransmis.

Le contrôle de flux garantit qu'un nœud transmetteur ne pourra pas saturer le nœud récepteur. La méthode la plus simple employée par TCP est l'utilisation d'un signal « non prêt » pour avertir l'unité émettrice de la saturation des tampons mémoires de l'unité réceptrice. Lorsque le récepteur peut accepter de nouvelles données, il envoie l'indicateur de transport «prêt».

Un accusé de réception positif avec retransmission est une autre technique employée par le protocole TCP pour garantir une transmission fiable des données. Si l'émetteur devait attendre un accusé de réception après l'envoi de chacun des paquets, le débit des données serait considérablement ralenti. Le fenêtrage est donc utilisé pour permettre la transmission de plusieurs paquets avant qu'un accusé de réception ne soit nécessaire. Les tailles de fenêtre TCP varient au cours de la durée de vie d'une connexion.

Un accusé de réception positif avec retransmission est une autre technique employée par le protocole TCP pour garantir une transmission fiable des données. Si l'émetteur devait attendre un accusé de réception après l'envoi de chacun des paquets, le débit des données serait considérablement ralenti. Le fenêtrage est donc utilisé pour permettre la transmission de plusieurs paquets avant qu'un accusé de réception ne soit nécessaire. Les tailles de fenêtre TCP varient au cours de la durée de vie d'une connexion.

Si aucun contrôle de flux et aucun accusé de réception ne sont requis pour une application, comme dans le cas d'une transmission de broadcast, le protocole UDP (*User Datagram Protocol*) peut remplacer le protocole TCP. UDP est un protocole de transport non orienté connexion de la pile de protocoles TCP/IP qui permet la simultanéité de plusieurs conversations, sans toutefois fournir d'accusés de réception ou de garantie de livraison. Un en-tête UDP est donc plus petit qu'un en-tête TCP du fait de l'absence des informations de contrôle.

Certains des protocoles et des applications opérant au niveau de la couche application sont bien connus des utilisateurs d'Internet:

- **Système DNS *(Domain Name System)*:** système utilisé dans les réseaux IP pour traduire le nom des nœuds du réseau en adresses IP.
- **Protocole FTP *(File Transfer Protocol)*:** protocole utilisé pour le transfert des fichiers entre les réseaux.
- **Protocole HTTP *(Hypertext Transfer Protocol)*:** protocole utilisé pour fournir des documents en langage HTML (*HyperText Markup Language*) à une application cliente, telle qu'un navigateur Web.
- **Protocole SMTP *(Simple Mail Transfer Protocol)*:** protocole permettant l'utilisation de services de messagerie électronique.
- **Protocole SNMP *(Simple Network Management Protocol)*:** protocole utilisé pour surveiller et contrôler les équipements du réseau, ainsi que pour gérer les configurations, la collecte de statistiques, les performances et la sécurité.
- **Telnet:** utilisé pour se connecter à un hôte distant sur lequel est exécutée une application serveur Telnet, puis pour exécuter des commandes depuis la ligne de commande.


Application
Transport
Internet
Accès
réseau